SANDIA REPORT
SAND2017-2384
Unclassified Unlimited Release
Printed March 2017

Technology Empowerment: Security Challenges

Drake Warren, George Backus, Wendell Jones, Thomas Nelson, Russ Skocypec

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@adonis.osti.gov
Online ordering:	http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.fedworld.gov
Online order:	http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2017-2384
Unclassified Unlimited Release
Printed March 2017

Technology Empowerment: Security Challenges

Drake Warren, George Backus, Wendell Jones, Thomas Nelson, Russ Skocypec

Systems Analysis and Decision Support
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0159

ABSTRACT

"Technology empowerment" means that innovation is increasingly accessible to ordinary people of limited means. As powerful technologies become more affordable and accessible, and as people are increasingly connected around the world, ordinary people are empowered to participate in the process of innovation and share the fruits of collaborative innovation. This annotated briefing describes technology empowerment and focuses on how empowerment may create challenges to U.S. national security. U.S. defense research as a share of global innovation has dwindled in recent years. With technology empowerment, the role of U.S. defense research is likely to shrink even further while technology empowerment will continue to increase the speed of innovation. To avoid falling too far behind potential technology threats to U.S. national security, U.S. national security institutions will need to adopt many of the tools of technology empowerment.

ACKNOWLEDGMENTS

We would like to thank the many people in Systems Analysis and Decision Support (150) who helped provide feedback on our presentations and our research. We would like to thank especially Cathy Ann Connelly, Chad Haddal, William Curtis, Richard Craft, Elizabeth Kistin Keller, and Howard Passell who all met with us regularly. Additionally, we would like to thank the subject matter experts from across Sandia that we consulted in the course of this research: Keith Yehle (163), Benn Tannenbaum (164), David Clauss (260), Warren Klein (260), Shawn Burns (263), Greg Hebner (1110), Haiqing Schwarz (1124), Sean Hearne (1132), Ben Cook (1910), Karla Weaver (1911), Allen Roach (2735), Dahlon Chu (5020), Barbara Funkhouser (5500), Phil Dreike (5700), John Sandusky (5944), Gary Laughlin (6020), Eric Vugrin (6921), Marcey Hoover (8040), and Steve Gossage (9336).

Contents

Figures

Tables

Nomenclature

3D	three-dimensional
AAAS	American Association for the Advancement of Science
CICADA	Close-In Covert Autonomous Disposable Aircraft
CRISPR	clustered regularly interspaced short palindromic repeats
CRR	Cyber Resilience Review
DARPA	Defense Advanced Research Projects Agency
DIUX	Defense Innovation Unit Experimental
DHS	Department of Homeland Security
DoD	Department of Defense
EU	European Union
FEMA	Federal Emergency Management Agency
FY	fiscal year
IED	improvised explosive device
JIEDDO	Joint Improvised Explosive Device Defeat Organization
MRAP	Mine-Resistant Ambush Protected
NSF	National Science Foundation
OECD	Organization for Economic Cooperation and Development
PCR	polymerase chain reaction
R&D	research and development
UAV	unmanned aerial vehicle
U.S.	United States
USA	United States of America

Glossary[1]

Empowerment	The giving of ability, power, and/or authority
Accessibility	The degree to which something can be obtained or used. (Ex: Handguns are more accessible in the United States than the United Kingdom.)
Affordability	The degree to which the financial costs of something are bearable
Connectivity	The degree to which an actor is connected to other actors
Technology	Knowledge and methods about the application of science[2]
Platform	Technologies that allow users to build and innovate[3]
Application	A specific use of the platform
Product	Something that has been produced—an application is a product of a platform
Innovation	Creation of something new or a new way of doing things (e.g., a new technology)
Resilience	The ability to function during and following a disruptive event (or set of events)[4]
Adaptability	The ability to learn how to do new things and innovate[5]

[1] Definitions based on dictionary definitions found in http://www.thefreedictionary.com and http://dictionary.reference.com, as well other sources noted below.

[2] This is a broad definition. Narrow definitions focus more on technology as physical concrete and physical rather than information-based.

[3] Based on Wittes and Blum (2015, p. 7).

[4] "Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is that system's ability to reduce efficiently both the magnitude and duration of the deviation from targeted system performance levels," (Biringer, et al, 2013, p. 107).

[5] "Instead of being really good at doing some particular thing, companies must be really good at learning to do new things," (Reeves and Deimler, 2011).

1 Background for Global Futures Series

As an outcome of the Sandia Lab Leadership Team's (LLT) strategic planning process, Center 0100 was asked to provide periodic one-hour information briefings on global futures (GF) relevant to Sandia. The intent was to create a discussion forum focused on GF, exploring possible implications for national security and Sandia's mission.
The briefings topics include:

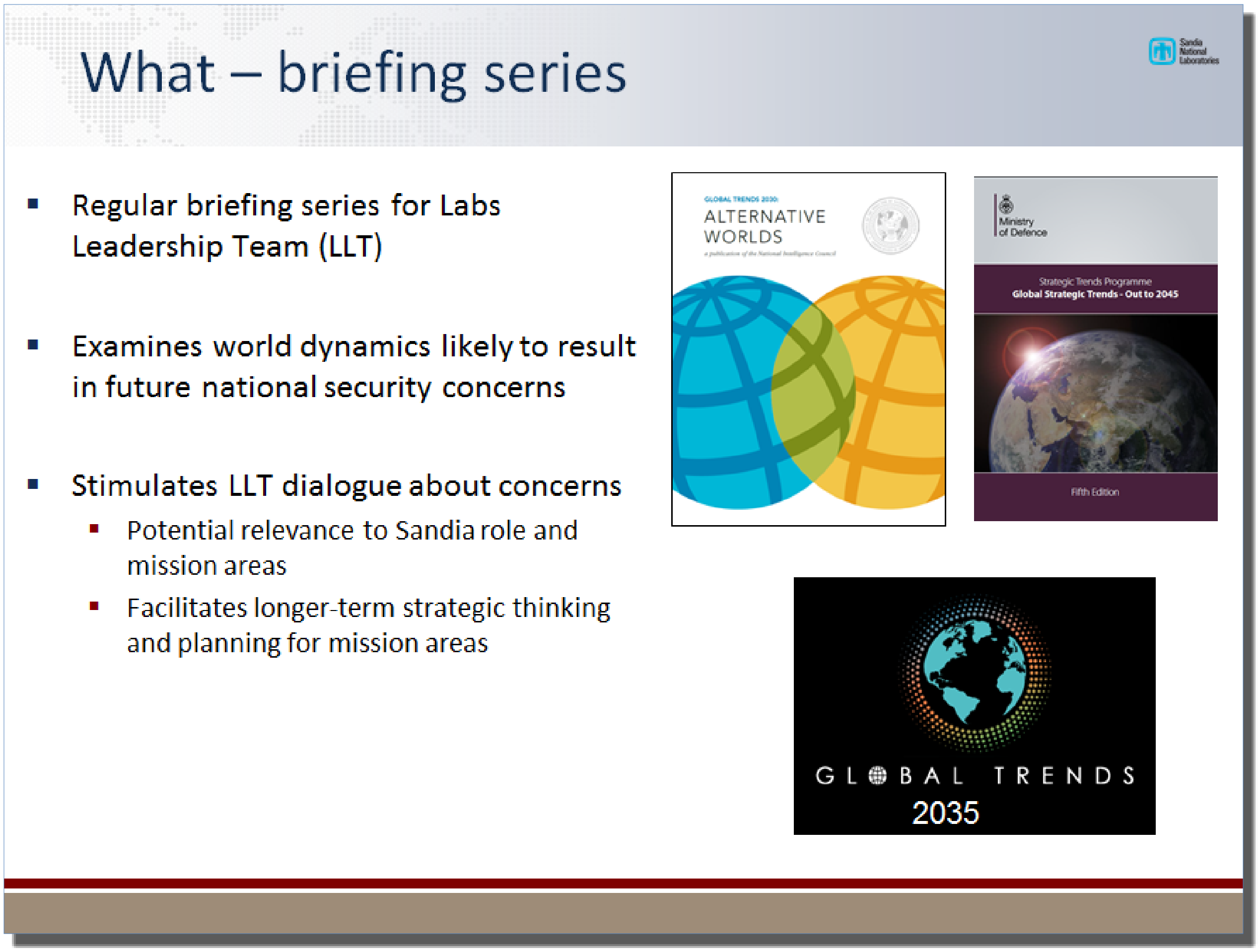
- Arctic Security
- Urbanization and Megacities
- Technology Empowerment (this report)
- Demographic and Economic Divergence
- Nonrenewable Resource Security

The method used to develop the series briefings was to survey diverse perspectives of realizable GF centered around a given topic area and identify the spectrum of resulting global implications. The rationale for the GF series of briefings research are presented in Figures 1 through 3.

Why – Sandia mission statement

The synergy and interdependence between our nuclear deterrence mission and broader national security missions forge a robust capability base and empower us to solve complex national security problems.

Figure 1. National Security Is Inherent in Sandia's Mission

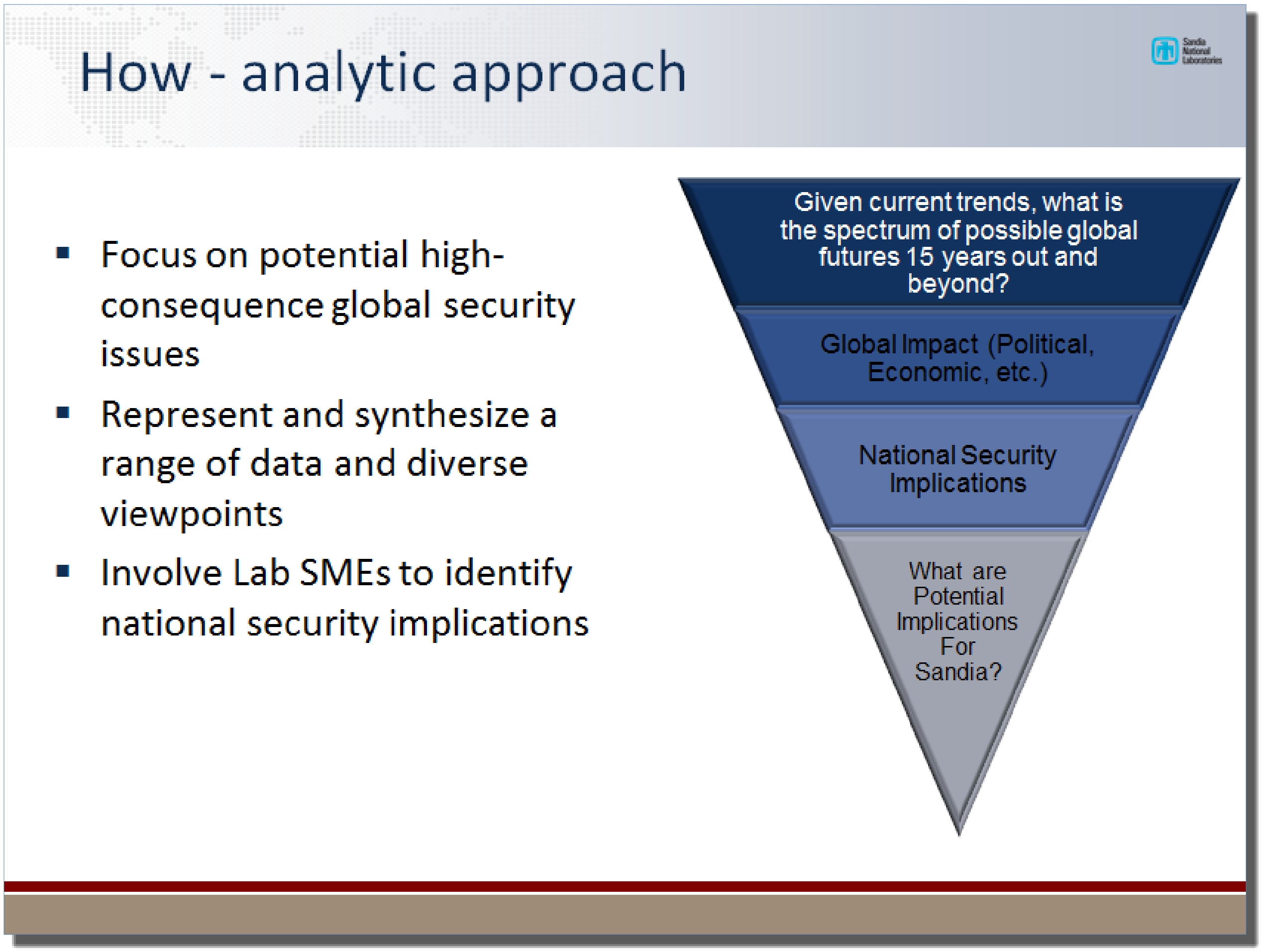


What – briefing series

- Regular briefing series for Labs Leadership Team (LLT)
- Examines world dynamics likely to result in future national security concerns
- Stimulates LLT dialogue about concerns
  - Potential relevance to Sandia role and mission areas
  - Facilitates longer-term strategic thinking and planning for mission areas

Sandia National Laboratories
GLOBAL TRENDS 2030:
ALTERNATIVE WORLDS
a publication of the National Intelligence Council
Ministry of Defence
Strategic Trends Programme
Global Strategic Trends - Out to 2045
Fifth Edition
GLOBAL TRENDS
2035

Figure 2. Purpose of the Series Briefing to Sandia Labs Leadership Team



How - analytic approach

- Focus on potential high-consequence global security issues
- Represent and synthesize a range of data and diverse viewpoints
- Involve Lab SMEs to identify national security implications

Given current trends, what is the spectrum of possible global futures 15 years out and beyond?

Global Impact (Political, Economic, etc.)

National Security Implications

What are Potential Implications For Sandia?

Figure 3. Sandia's Analytic Approach to Global Security

1.1 Introduction to Technology Empowerment

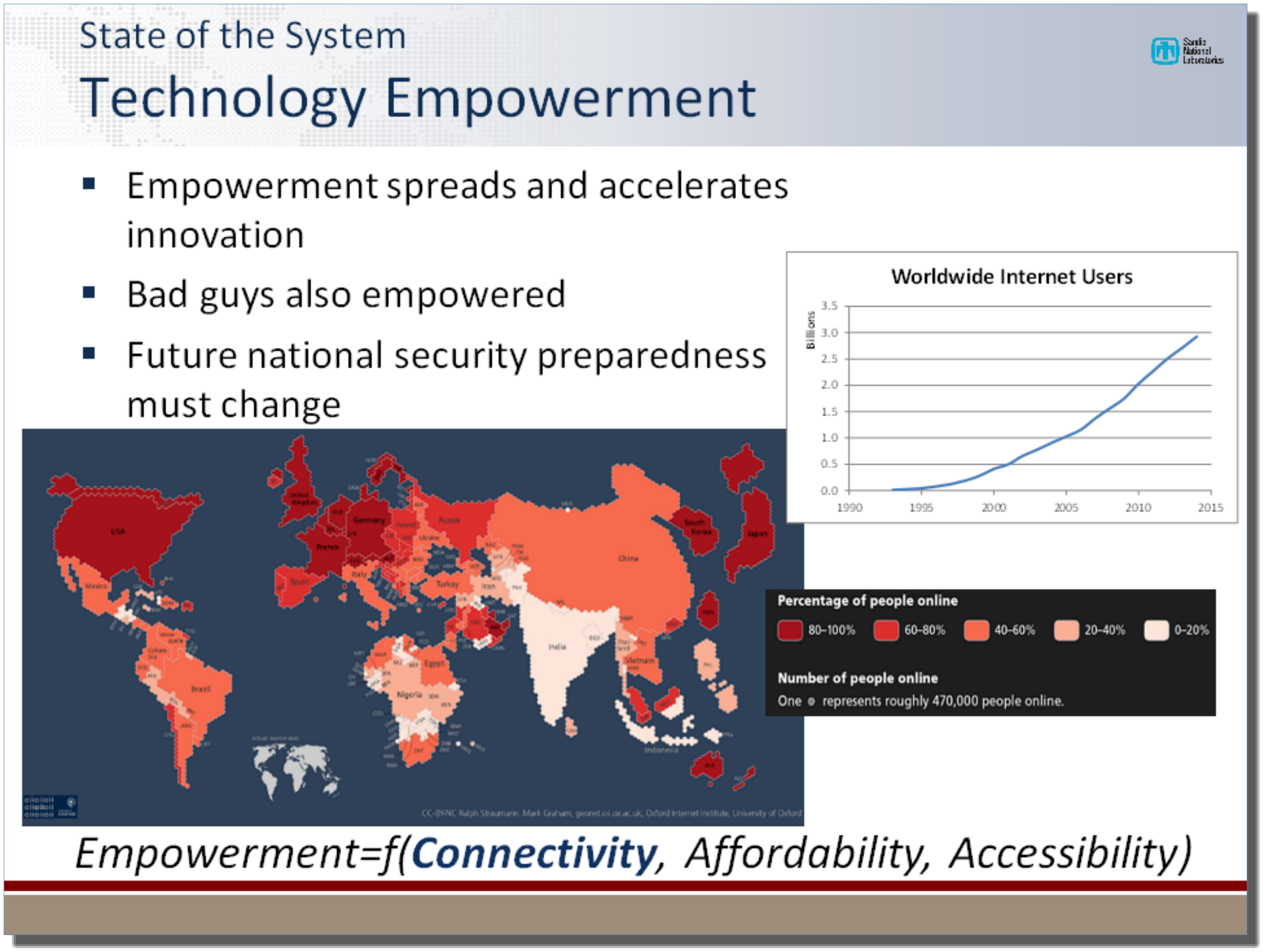
Technology empowerment is placing innovation in the hands of ordinary people with relatively few resources. Empowerment is allowing these people not only to obtain the fruits of this innovation, but also to participate in innovation themselves. Empowerment increases the pace and impact of innovation by making innovation available to so many people.

This report discusses the implications of increases in technology empowerment. There are many impacts of this empowerment, many of which are likely to be beneficial to society. We focus on some of the risks of this empowerment. Actors with interests counter to the United States will also be empowered, which will present future challenges to U.S. national security.
The changing landscape of innovation coupled with increased threats from empowerment mean that U.S. national security policy and preparedness must change in the future to avoid falling too far behind threats exacerbated by technology empowerment. This briefing will discuss some ways in which U.S. national security may be impacted by empowerment, and how policy might change in the future.

2 State of the System

We view empowerment as a function of three drivers, all of which are closely related but have unique connotations. Each of these drivers has been strengthening and each is likely to increase in the future, thereby empowering more people with increasingly powerful technology.

2.1 Connectivity



State of the System

Technology Empowerment

- Empowerment spreads and accelerates innovation
- Bad guys also empowered
- Future national security preparedness must change

*Empowerment=f(**Connectivity**, Affordability, Accessibility)*

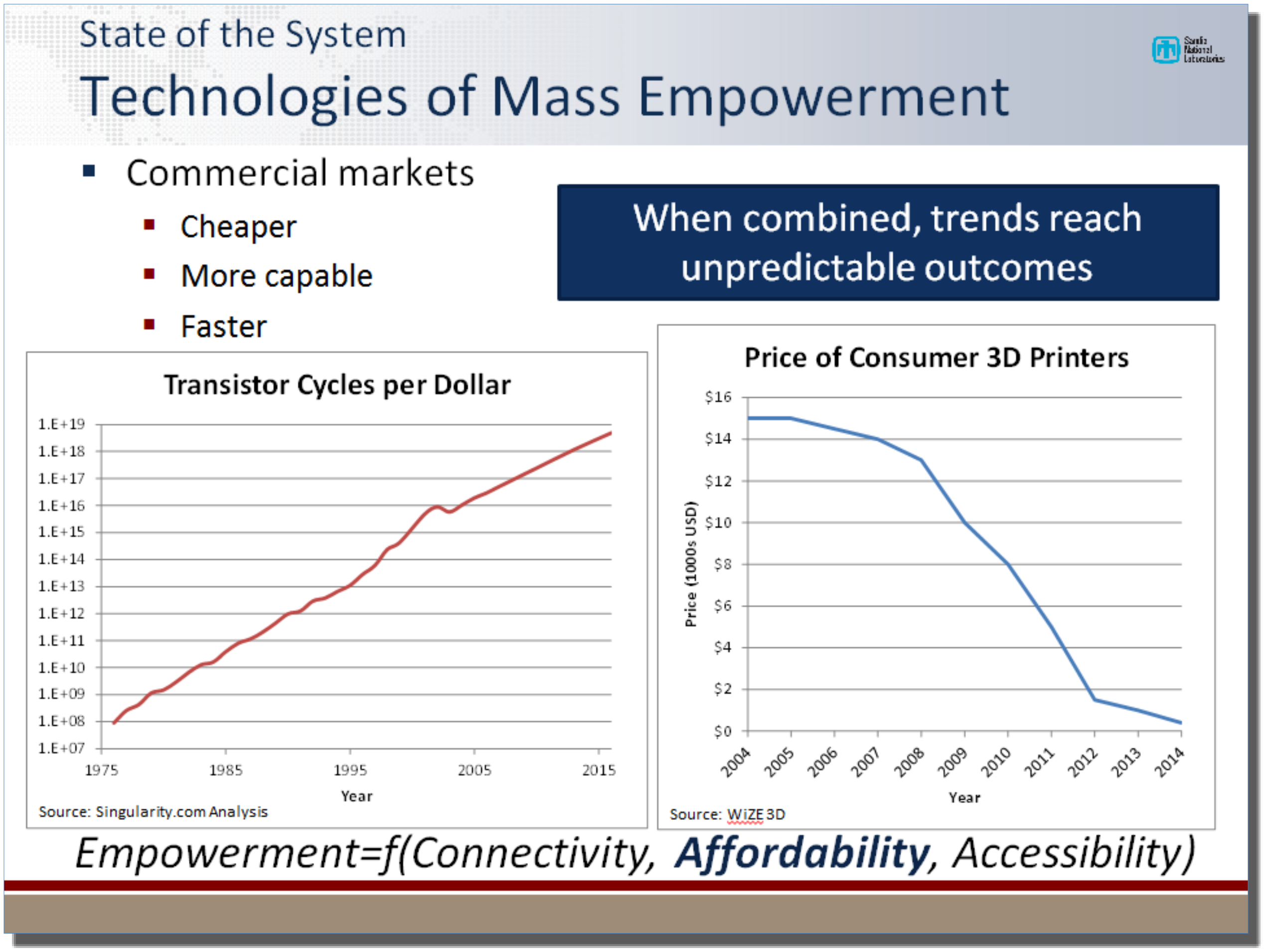
Figure 4. Technology Empowerment—Connectivity

Connectivity is the degree to which an actor is connected to other actors. Connectivity is a necessary condition for empowerment. In the last two decades connectivity has increased tremendously through the spread of the Internet. As Figure 4 shows,[6] nearly all people in most developed nations use the Internet. This has resulted in rapid growth in Internet use since 2000.[7] This growth is likely to continue into the future as Internet use spreads globally, particularly to developing countries, thereby creating the prerequisites for empowerment across the globe.

[6] The map is from http://www.itproportal.com/2015/07/10/world-map-resized-to-show-internet-adoption-by-country/.

[7] Data for Internet users from Internet Live Stats (elaboration of data by International Telecommunication Union and United Nations Population Division.

2.2 Affordability



State of the System

Technologies of Mass Empowerment

- Commercial markets
  - Cheaper
  - More capable
  - Faster

When combined, trends reach unpredictable outcomes

Transistor Cycles per Dollar

Source: Singularity.com Analysis

Price of Consumer 3D Printers

Source: WiZE 3D

Empowerment=f(Connectivity, ***Affordability****, Accessibility)*

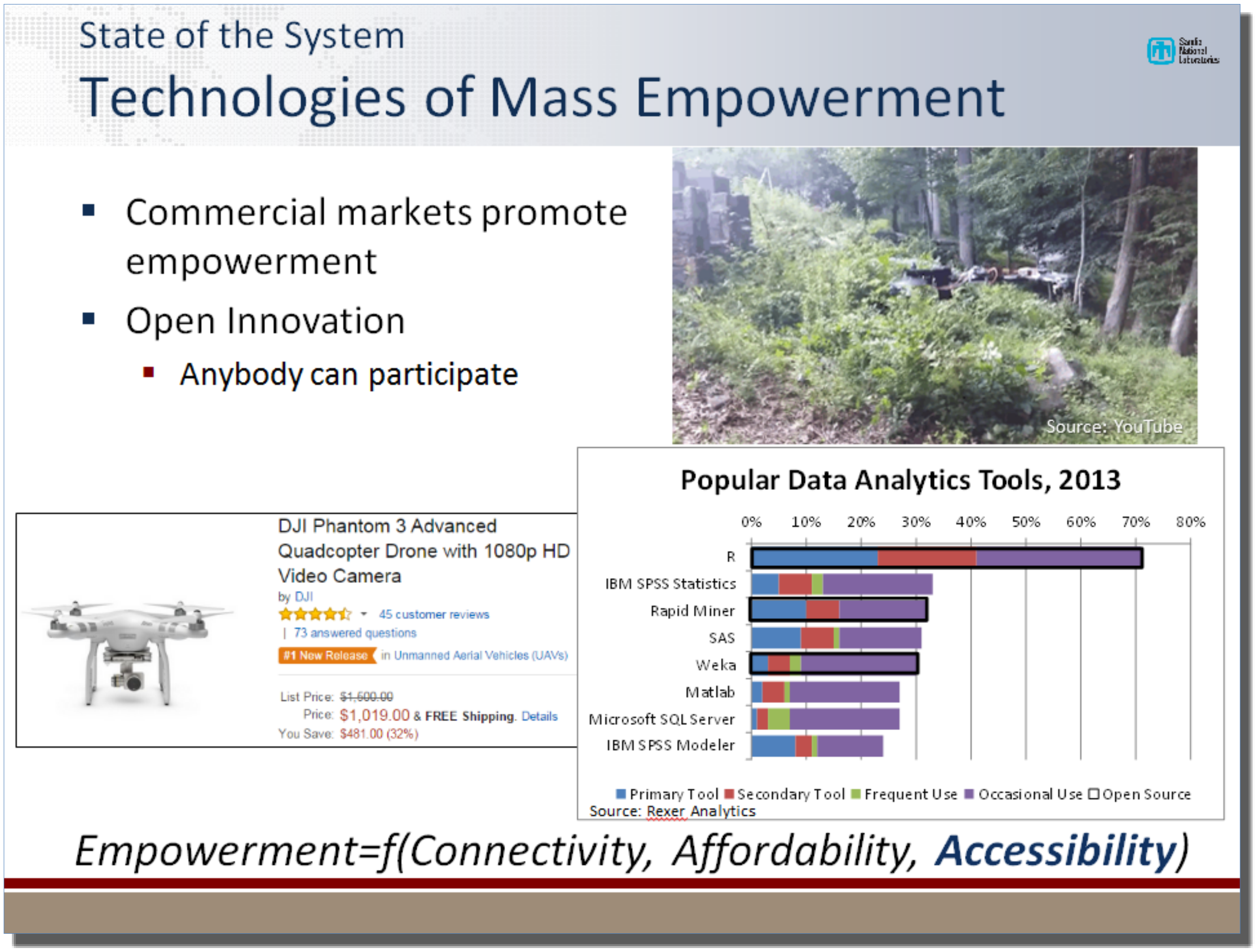
Figure 5. Technology Empowerment—Affordability

The second driver of technology empowerment is affordability. Commercial markets help drive technology to become cheaper, more capable, and increase the pace of innovation. This means that consumers can afford an ever increasing bang for the buck.

We looked at a number of trends in prices, which show similar patterns of increasing capability and decreasing cost (Figure 5).[8] In isolation, each of these trends seems to increase the performance of capabilities that people can afford. In combination and with connectivity and accessibility, however, these "modern technologies of mass empowerment" (Wittes and Blum, 2015) result in unpredictable surprises that radically change the types of capabilities that ordinary people can invent and acquire.

[8] Microprocessor Cost per Transistor Cycle graph is based off an analysis by Singularity.com (http://www.singularity.com/charts/page62.html, accessed August 4, 2015). Price of Consumer three-dimensional (3D) printers is from http://www.wize3d.com/history-of-3d-printing/ (accessed August 4, 2015).

2.3 Accessibility



State of the System

Technologies of Mass Empowerment

- Commercial markets promote empowerment
- Open Innovation
  - Anybody can participate

Source: YouTube

DJI Phantom 3 Advanced Quadcopter Drone with 1080p HD Video Camera

by DJI

45 customer reviews | 73 answered questions

#1 New Release in Unmanned Aerial Vehicles (UAVs)

List Price: ~~$1,600.00~~

Price: $1,019.00 & FREE Shipping. Details

You Save: $481.00 (32%)

Popular Data Analytics Tools, 2013

Source: Rexer Analytics

Empowerment=f(Connectivity, Affordability, ***Accessibility****)*

Figure 6. Technology Empowerment—Accessibility

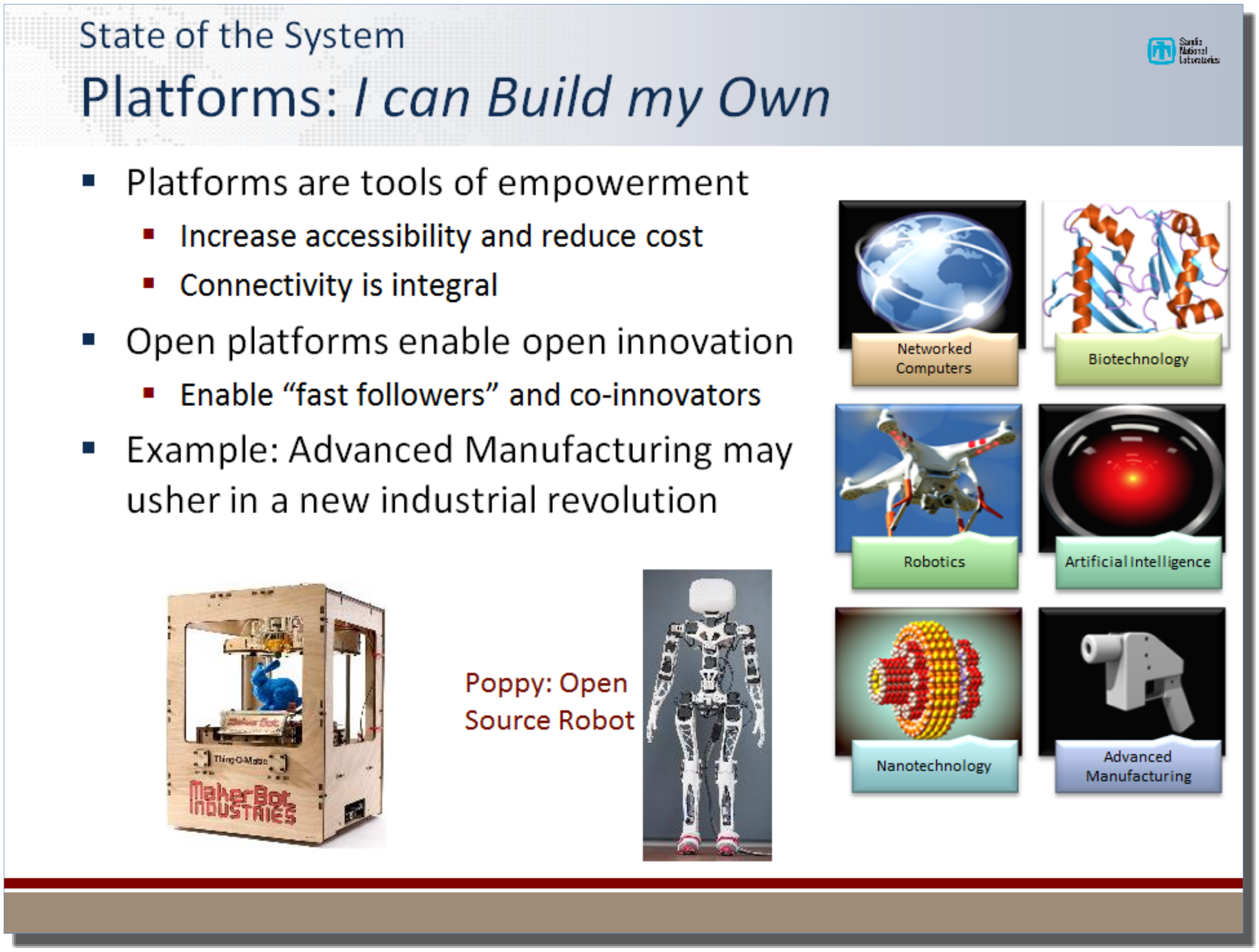
An example of the surprise that empowerment creates when connectivity and affordability combine with accessibility is illustrated by the case of Austin Haughwout, an 18-year old mechanical engineering student and drone enthusiast from Connecticut who created a “flying gun.” He had access to a handgun and access to unmanned aerial vehicle (UAV) technology. For example, capable UAVs can be purchased from retailers like Amazon.com[9] for only a few hundred to a thousand dollars (Figure 6). He combined the UAV and handgun and showed the world a demonstration of the technology on YouTube[10]. By sharing the video, Haughwout not only showed off his creation, but he planted the seeds for others to build on his innovation. In the future, further advances in flying guns are likely to result from the process of open innovation where enthusiasts like Haughwout build on the ideas of others and share the results of their efforts to the world.

[9] The Amazon.com screen capture is from search results on July 21, 2015. As of November 2, 2016, the same model with an improved camera is available for $748.01.

[10] The video is available at https://www.youtube.com/watch?v=xqHrTtvFFIs (by Austin Haughwout, aka “Hogwit”). The image is a screen capture from http://ak-hdl.buzzfed.com/static/2015-07/16/11/enhanced/webdr07/anigif_enhanced-21347-1437061286-27.gif.

An example of accessibility that is familiar to many in the research and development (R&D) world is open source software. As shown in the graph above,[11] the open-source software called *R* is by far the most widely adopted statistical analysis package in use today. It is not only free, but it is extremely capable because so many researchers have developed R tools and shared them over the Internet that anybody conducting statistical research can easily build off of the work of others. Unlike most commercial software, if the previously developed routines in *R* do not fit their precise needs, *R* users have the ability to modify the source code. Once a user has created new *R* packages by combining others' packages and their own code, they can share their work to other *R* users. Thus, this accessibility perpetuates a positive feedback cycle in which users leverage others' work and *R* becomes an increasingly powerful research tool.

2.4 Platforms



State of the System

Platforms: *I can Build my Own*

- Platforms are tools of empowerment
  - Increase accessibility and reduce cost
  - Connectivity is integral
- Open platforms enable open innovation
  - Enable "fast followers" and co-innovators
- Example: Advanced Manufacturing may usher in a new industrial revolution

Poppy: Open Source Robot

Networked Computers

Biotechnology

Robotics

Artificial Intelligence

Nanotechnology

Advanced Manufacturing

Figure 7. Platforms as Tools of Empowerment

Platforms like *R* provide users with the tools and technologies to build their own products and applications (Figure 7). Platforms increase connectivity, affordability, and accessibility, thus the widespread adoption of common platforms is a key driver of technology empowerment.

[11] Data for the graph above are from Rexer Analytics: https://r4stats.files.wordpress.com/2012/04/rexeranalytics2013.png.

The most well-known example of such a platform is the Internet, but many other instances of networked computers also serve as such platforms (e.g., open-source software like *R*, Microsoft Windows, and iPhones). Some other broad platforms that are likely to be important in the future are biotechnology[12], robotics, artificial intelligence, nanotechnology, and advanced manufacturing.[13,14]

Platforms enable actors to be "fast followers"[15] by quickly adopting—at relatively low cost—others' innovations. In the past, the focus on products (as well as closed platforms) meant that new entrants to innovation ecosystems took a longer time to build a knowledge base necessary to access the innovations that others had already developed but kept secret, hidden, or inaccessible. With open platforms, new entrants can more quickly access these innovations and quickly start contributing to innovation themselves.

Advanced manufacturing appears to be a platform that is particularly likely to change the world for R&D organizations.[16] Marsh (2012) calls this the "Fifth Industrial Revolution" as mass

[12] The picture of biotechnology in the box is of clustered regularly interspaced short palindromic repeats (CRISPR), which may prove to be a particularly impactful platform. In just three years gene editing has been revolutionized to become low cost and highly accessible. CRISPR is described as being much like polymerase chain reaction (PCR), which revolutionized the accessibility and affordability of reading genomes, but for editing genomes rather than just reading them (Ledford, 2015). Biotechnology is discussed in depth in a subsequent Global Futures study (Sumner, et al. 2016).

[13] Wittes and Blum (2015) discuss, in depth, the importance of platforms. They highlight Networked Computers, Biotechnology, Robotics, and Nanotechnology as important platforms in the future. We also added artificial intelligence (which may be viewed as a subcategory of networked computers) and advanced manufacturing.

[14] Image credits:

Networked Computers: By The people from the Tango! project (The Tango! Desktop Project) [Public domain or Public domain], via Wikimedia Commons; https://upload.wikimedia.org/wikipedia/commons/7/70/Applications-internet.svg.

Biotechnology: (CRISPR Protein) "PDB 1wj9 EBI" by Jawahar Swaminathan and MSD staff at the European Bioinformatics Institute - http://www.ebi.ac.uk/pdbe-srv/view/images/entry/1wj9600.png, displayed on http://www.ebi.ac.uk/pdbe-srv/view/entry/1wj9/summary. Licensed under Public Domain via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:PDB_1wj9_EBI.jpg#/media/File:PDB_1wj9_EBI.jpg; https://en.wikipedia.org/wiki/CRISPR#/media/File:PDB_1wj9_EBI.jpg.

Robotics: This is a close up view of the drone being flown by this operator NT4936: Flying a drone at Ladhope Recreation Ground. © Copyright Walter Baxter and licensed for reuse under this Creative Commons License. http://www.geograph.org.uk/reuse.php?id=4487469.

Artificial Intelligence: "HAL9000" by Cryteria - Own work. Licensed under CC BY 3.0 via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:HAL9000.svg#/media/File:HAL9000.svg.

Nanotechnology: Hypothetical nano-gear system. "Nanob". Licensed under CC BY-SA 3.0 via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Nanob.jpg#/media/File:Nanob.jpg.

Advanced Manufacturing: Liberator printed pistol. "DDLiberator2.3" by Kamenev - Own work. Licensed under CC BY-SA 3.0 via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:DDLiberator2.3.jpg#/media/File:DDLiberator2.3.jpg.

[15] For example in the military, "fast followers (i.e., military organizations oriented toward a commercial-first mindset) earn the opportunity to capitalize on superior capabilities more quickly and at a comparatively lower cost" (Harrison et al., 2015, p. 33).

[16] There appears to be wide agreement that advanced manufacturing will be important in the future, but disagreement over the timing. For example, the Defense Science Board (2013) believes that advanced manufacturing will change defense, but it thinks these impacts are far into the future, thus justifying hedging investments (i.e., increasing familiarity with the platform and searching for future uses) rather than major investments.

production is replaced by “mass customization” and “mass personalization”. He believes that this will result in tremendous opportunities for skilled designers with diverse skills who can design niche applications, while it may further erode employment in pure manufacturing (much of which has already left the United States).

Advanced manufacturing is likely to have a substantial impact on logistics as the need to ship goods as they move through supply-chains is reduced. Further, advanced manufacturing will enable detailed records of how each product was produced, which can be used to better anticipate and diagnose problems and simulate the behavior of individual products (Chief Scientist of the United States Air Force, 2013).

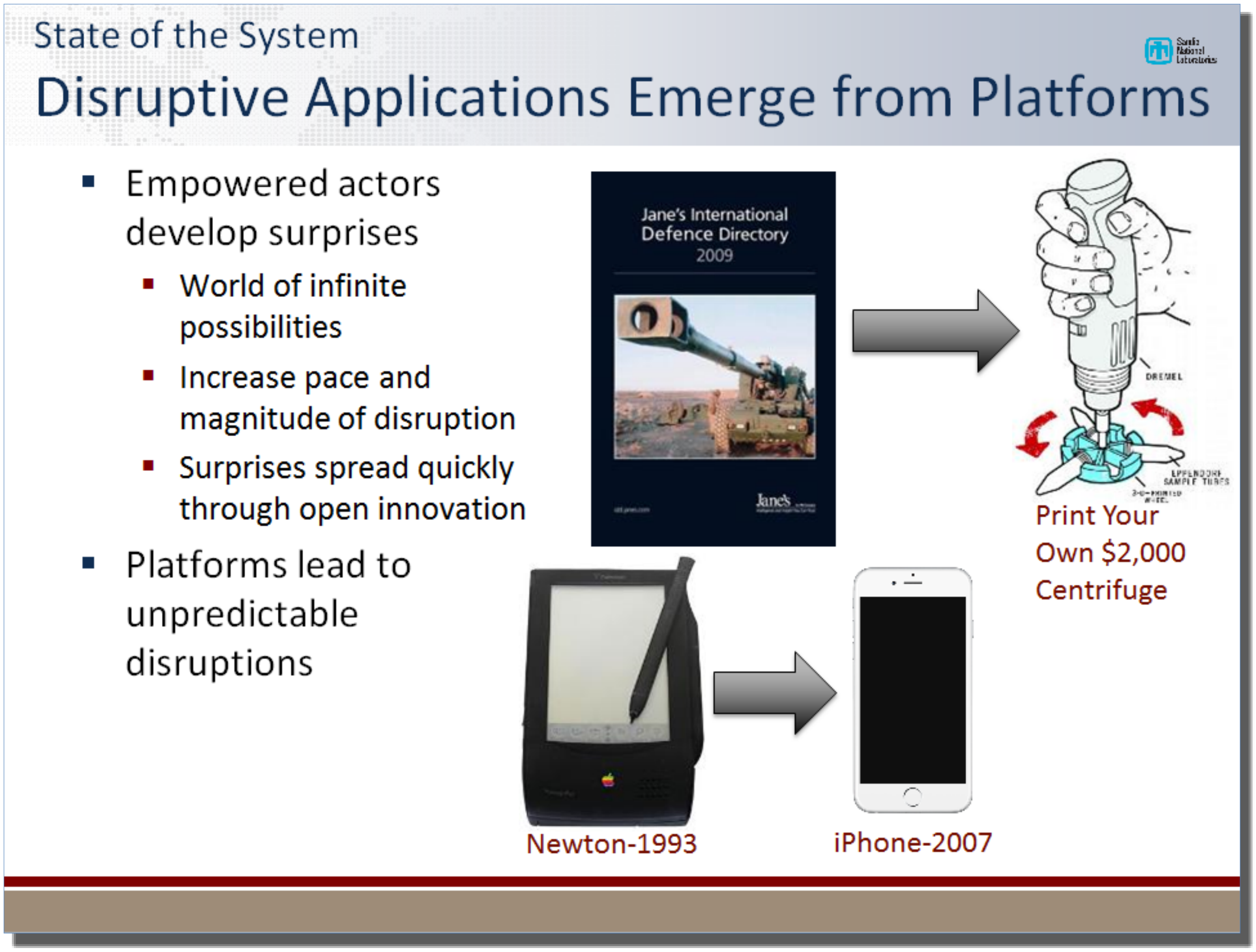
Advanced manufacturing available to consumers is still relatively primitive, but it is quickly becoming increasing capable.[17] This means that advanced manufacturing is likely to help drive manufacturing from “produc[ing] very large numbers of moderately capable systems as compared to the current expectation of producing small numbers of exquisitely capable systems” (Defense Science Board, 2013, p. 72).

In the future, advanced manufacturing will likely enable people to print just about anything from a 3D desktop printer.[18] Instead of ordering things online and having them shipped from a retailer like Amazon.com, people may order things from a retailer who will transmit the design to the home 3D printer. In addition, open-source design (like the Poppy robot project) is likely to become more popular, which will allow people to customize products for their own needs and share their innovations with others in much the same manner that open-source software is shared today. This increased digitization and empowerment of manufacturing will have implications to national security (which we discuss more broadly in the next section). For example, designs will be difficult to trace and impossible to control since they will be spread across the Internet. Further, malicious designs may be able to engineer backdoors and weak links into designs that can be exploited and attacked similar to cyber vulnerabilities.

[17] For example, the Makerbot came out in 2010 for around $1000 and could produce objects like plastic rabbits. "Makerbot Thing-O-Matic Assembled Printing Blue Rabbit" by Makerbot Industries - Makerbot Flikr. Licensed under CC BY 2.0 via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Makerbot_Thing-O-Matic_Assembled_Printing_Blue_Rabbit.jpg#/media/File:Makerbot_Thing-O-Matic_Assembled_Printing_Blue_Rabbit.jpg. But even relatively simple printers can be used to make pieces to construct more complicated systems, such as the Poppy open-source robot project "Open-Source 3D printed Poppy humanoid robot" by Inria / Poppy-project.org / Photo H. Raguet. - http://phototheque.inria.fr/phototheque/search.do?q=poppy. Licensed under CC BY-SA 4.0 via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Open-Source_3D_printed_Poppy_humanoid_robot.jpg#/media/File:Open-Source_3D_printed_Poppy_humanoid_robot.jpg.

[18] For example, “molecular-level manufacturing” could combine advanced manufacturing with nanotechnology to combine different types of materials at the molecular level (Gold, 2014).

2.5 Tech-Application Surprise[19]



State of the System

Disruptive Applications Emerge from Platforms

- Empowered actors develop surprises
  - World of infinite possibilities
  - Increase pace and magnitude of disruption
  - Surprises spread quickly through open innovation
- Platforms lead to unpredictable disruptions

Print Your Own $2,000 Centrifuge

Newton-1993

iPhone-2007

Jane's International Defence Directory 2009
Jane's
DREMEL
EPPENDORF SAMPLE TUBES
3-D-PRINTED WHEEL

Figure 8. Emergent Disruptive Applications

In the past, people needed access to substantial resources to participate meaningfully in many innovation processes. For example, national laboratories provide substantial equipment, personnel, and funding for conducting R&D. In many areas, innovations will still benefit from access to these resources, especially in areas like space and nuclear research that require large capital investments. However, in an increasing number of areas newly empowered actors with few resources will be central to innovation. Since the world has infinite possibilities, the multiplication of empowered people and organizations participating in innovation ecosystems will result in an explosion of surprises that increase the pace and magnitude of disruption. We

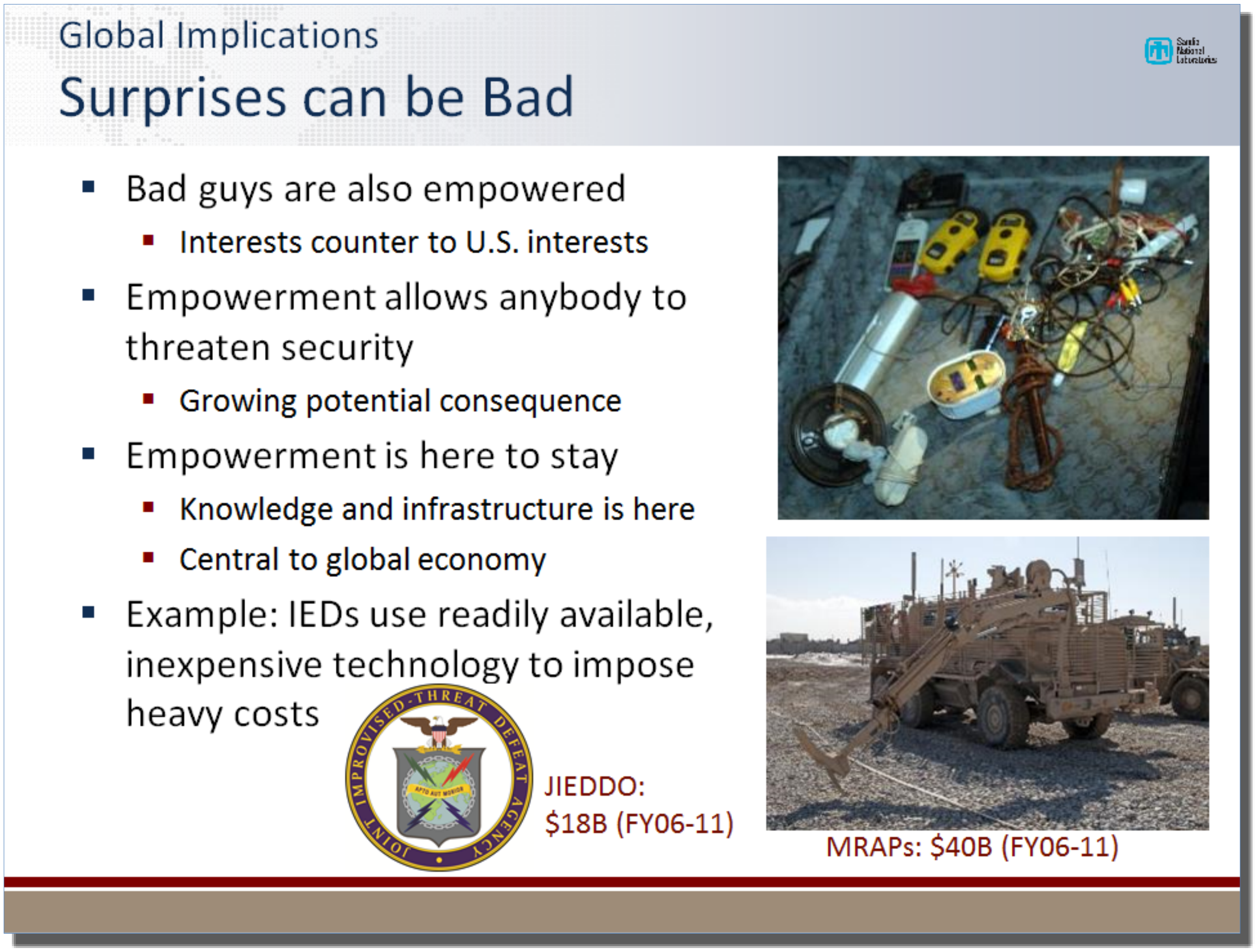
[19] Image credits: **DremelFuge**: Daniel Grushkin, 2013, "How to Build Your Own DIY Centrifuge: Get a Lab-Grade Centrifuge (Normally $2,000) for 50 Bucks", *Popular Science*, August 16, 2013, http://www.popsci.com/diy/article/2013-07/how-build-your-own-diy-centrifuge.
Newton: "Apple Newton-IMG 0454-cropped" by Photograph by Rama, Wikimedia Commons, Cc-by-sa-2.0-fr. Licensed under CC BY-SA 2.0 fr via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Apple_Newton-IMG_0454-cropped.jpg#/media/File:Apple_Newton-IMG_0454-cropped.jpg.
iPhone: "IPhone6 silver frontface" by Rayukk at English Wikipedia. Licensed under CC BY-SA 3.0 via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:IPhone6_silver_frontface.png#/media/File:IPhone6_silver_frontface.png.

call these *tech-application surprises* since they tend to the surprising applications of existing technology or platforms.
Technology and innovation disruptions are often created through "the power of unconventional and unconstrained imagination" (Naval Research Advisory Committee, 2009). Disruptive innovations often arise from creative applications that leverage existing, widely available technology, thus innovation does "need not be radical or novel from an engineering or technical point of view." (Committee on Forecasting Future Disruptive Technologies, National Research Council, 2009, p. 34). A common belief is that innovation in today's world of empowerment is less about "entirely novel breakthroughs" and more about "the clever combination and extension of existing ideas" (The Economist, 2015d).

A useful example that illustrates the importance of platforms is the Apple Newton/iPhone example, in 1994 Apple released the Newton, a type of handheld computer that never achieved a high level of popularity. In 2007 Apple issued the iPhone, which caught on and changed the world—smart phones are now ubiquitous. The Newton and iPhone are similar ideas, although the iPhone has about 15 years of newer technology and a more pleasing design. However, the key difference is probably that the iPhone leveraged platforms. The iPhone allowed easy, anytime access to the Internet, which had exploded in popularity since 1994. Perhaps more importantly, the iPhone itself became a platform to which application developers gravitated. The adoption of the iPhone as a platform (as well as its Android competitor shortly thereafter) has led to a number of potentially world-changing applications. For example, Uber has changed the taxi industry, and it (or similar apps) has the potential to change the way we own (or rent) automobiles in the future—especially as autonomy expands.

Open platforms also help to create tech-application surprise because they bring together a wide variety of co-innovators. In the past, innovation often occurred in a closed system in which people worked with a small group of people. Now, innovation networks are more often large, open networks, which network researchers believe enhances creativity and innovation success (Simmons, 2015).

3 Global Implications



Global Implications

Surprises can be Bad

- Bad guys are also empowered
  - Interests counter to U.S. interests
- Empowerment allows anybody to threaten security
  - Growing potential consequence
- Empowerment is here to stay
  - Knowledge and infrastructure is here
  - Central to global economy
- Example: IEDs use readily available, inexpensive technology to impose heavy costs

JIEDDO: $18B (FY06-11)

MRAPs: $40B (FY06-11)

JOINT IMPROVISED-THREAT DEFEAT AGENCY
Sandia National Laboratories

Figure 9. Adversaries Also Empowered

There are many implications of technology empowerment to economies and societies around the world. In this section, we focus on security implications. Our examples are focused on security implications to the United States, but the general implications are broadly applicable.

3.1 Some Technology Empowerment Surprises may be Undesirable[20]

Today's open innovation ecosystem not only powers the economy—it also empowers actors that have interests contrary to states' interest. Technology empowerment creates security risks.
A prime example of bad surprises that is familiar to the U.S. national security community is improvised explosive devices (IEDs) used against U.S. forces (Figure 9). IEDs use relatively simple technology that bomb makers obtain legitimately. The "open innovation" of the bomb

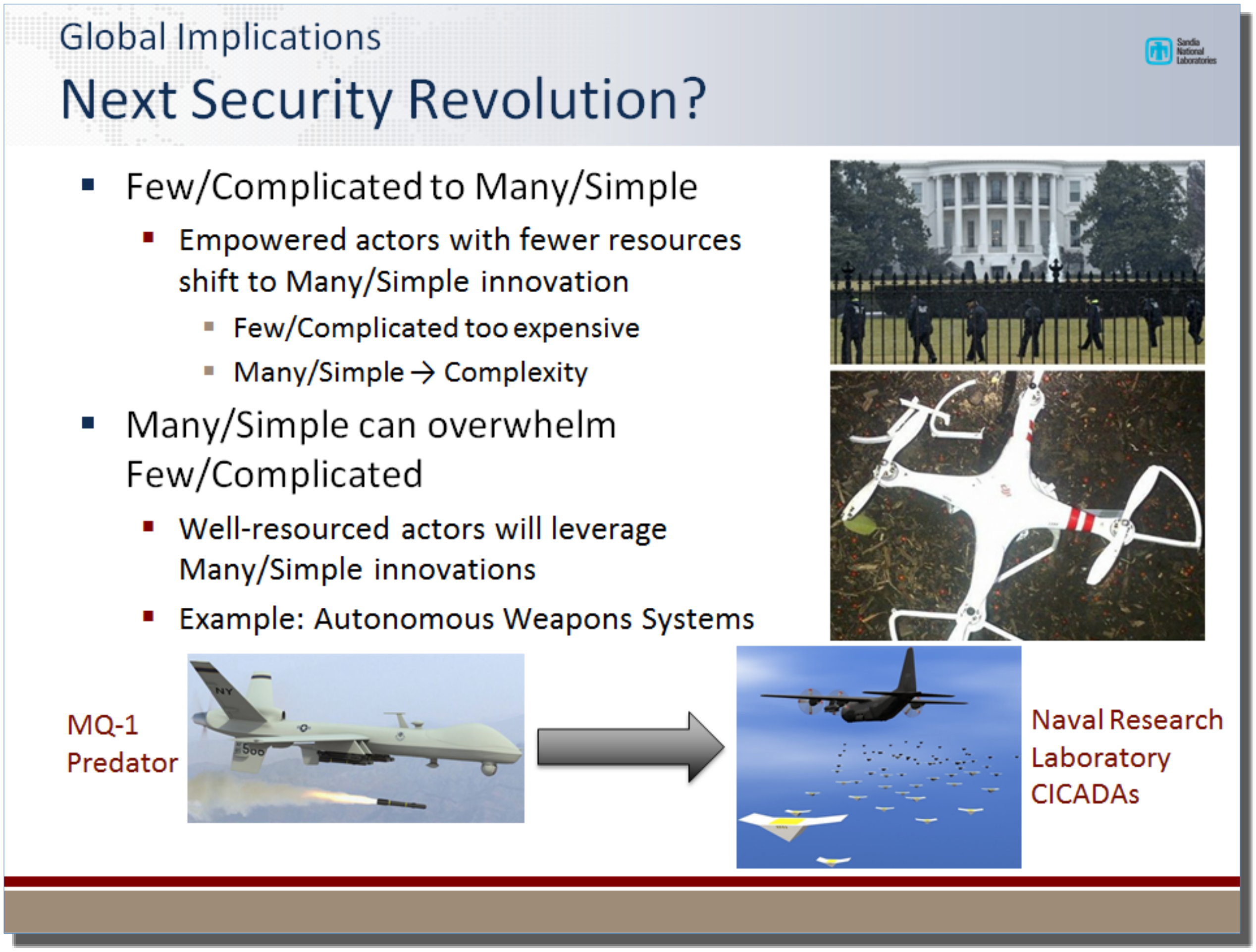
[20] Image Credits: **Suitcase IED**: US Army News Service: http://usarmy.vo.llnwd.net/e2/-images/2010/12/16/94940/size0-army.mil-94940-2010-12-17-071208.jpg, http://www.army.mil/article/49580/how-fast-can-counter-ied-tools-be-fielded/.
Buffalo MRAP: Sgt. Christopher McCullough, US Army News Service, https://www.army.mil/article/88382/Keeping_the_roads_of_Afghanistan_safe__one_IED_at_a_time, https://www.army.mil/e2/c/images/2012/10/02/266102/size0.jpg.
JIEDDO Seal: https://www.jieddo.mil/images/JIEDDO_Seal_1147.jpg.

making community, facilitated through communications (i.e., the Internet) enables bomb makers to discover highly effective, innovative ways of designing and deploying IEDs (Joint Improvised Explosive Device Defeat Organization [JIEDDO], 2012). The United States spent large amounts of money,[21] while thousands of lives were lost, to try to counter IEDs. However, open innovation helped U.S. adversaries counter U.S. efforts and disseminate these innovations. Like many threats that will emerge from technology empowerment, the use of IEDs could never be completely prevented or defeated; instead, it had to be managed.

There is no way to "undo" empowerment to mitigate the risk of technology empowerment of adversaries. Once empowered, it would be nearly impossible to return to a world without empowerment. The knowledge is out and cannot be recalled. Further, the infrastructure (e.g., the Internet) is in place and economies rely on empowerment for their functioning.

[21] Estimates of counter-IED spending are from Government Accountability Office (2012).

3.2 From Few and Complicated to Many, Simple, and Complex[22]



Global Implications

Next Security Revolution?

- Few/Complicated to Many/Simple
  - Empowered actors with fewer resources shift to Many/Simple innovation
    - Few/Complicated too expensive
    - Many/Simple → Complexity
- Many/Simple can overwhelm Few/Complicated
  - Well-resourced actors will leverage Many/Simple innovations
  - Example: Autonomous Weapons Systems

MQ-1 Predator

Naval Research Laboratory CICADAs

Figure 10. Many and Simple

Militaries often focus their investments on complicated systems to gain an asymmetric advantage in capabilities over potential adversaries (Figure 10). Complicated systems are very expensive, so nations like the United States that have large financial resources have an advantage. Over time, these systems have increased in expense, thereby causing the quantity of purchases to decrease. Norm Augustine recognized this trend in 1979 when he projected that the entire defense budget in 2054 would buy a single tactical aircraft (Augustine, 1979). In 2015, Augustine looked again at trends in price and quantity and projected that this milestone would be reached on July 23, 2054 (Augustine, 2015).

The increasing expense of complicated systems, therefore, is not a new trend. However, recent trends fueling empowerment have been increasing the affordability of many technologies for

[22] **White House drone**: http://www.theatlantic.com/politics/archive/2015/01/beware-the-drones-white-house-obama/384869/.
Predator Drone: http://twt-thumbs.washtimes.com/media/image/2014/05/08/predator-firing-missile4_s878x659.jpg?05ff56987ef8faa35b1aa0fda305c1c1f5574c93.
Naval Research Laboratory Cicada: http://www.washingtonpost.com/news/innovations/wp/2015/05/20/cicadas-locusts-and-the-new-innovation-of-military-infestations/.

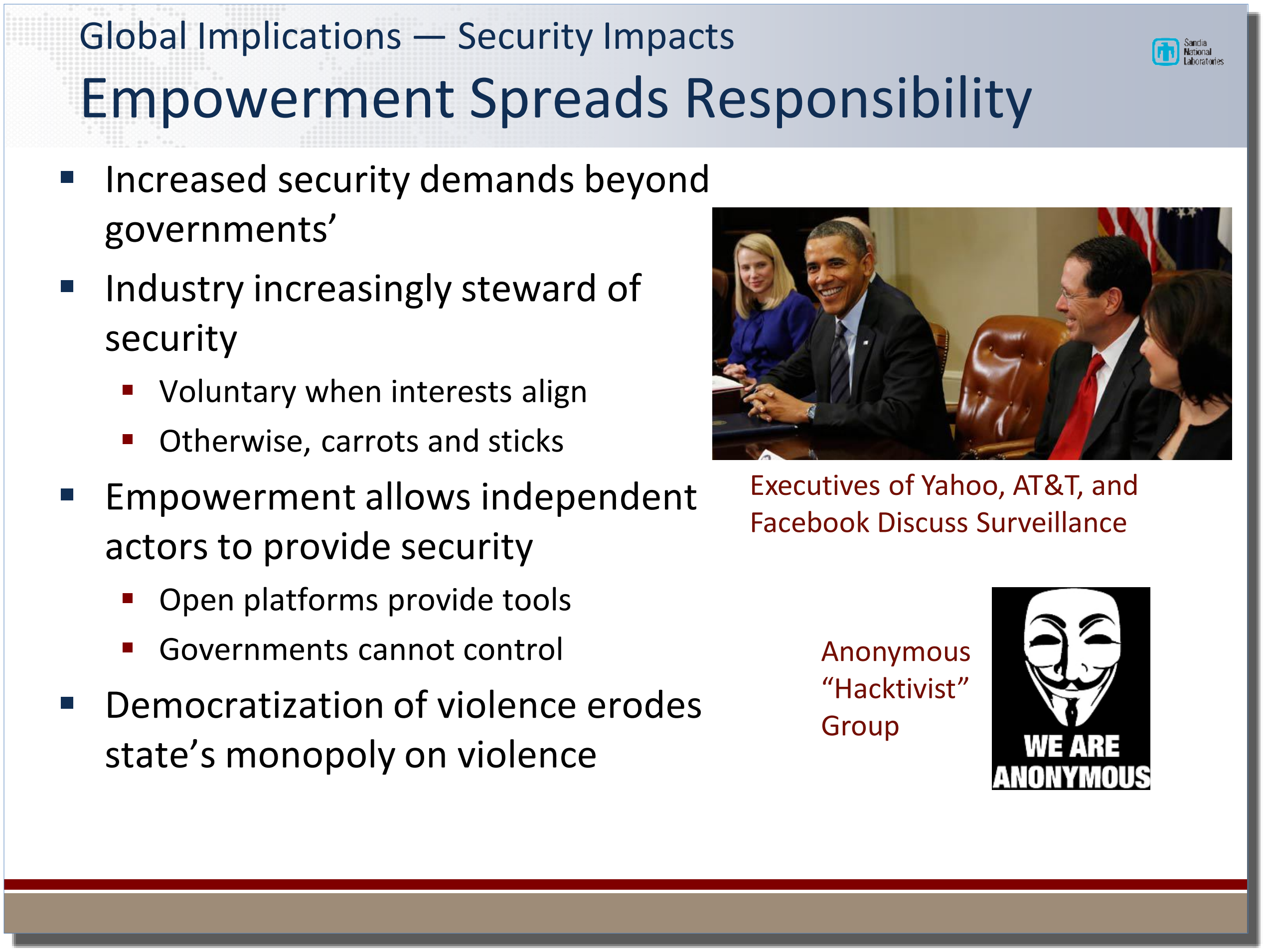
actors with relatively few resources, while drastically increasing the pace, magnitude, and spread of innovation. Empowerment is favoring the many and simple over the few and complicated.

The future of warfare, in turn, might rest on this shift to the many and simple (see Hammes, 2014). There are two main drivers of this shift. First, with the turn to many and simple, the environment grows increasing complex. As noted by complexity researchers (e.g., Carlson and Doyle, 2002), complicated systems can be extremely fragile when exposed to environments that were not anticipated when the systems were designed. Empowerment helps adversaries to discover such environments. Thus few and complicated military systems are increasingly vulnerable to the many and simple, as was clearly illustrated by the United States' difficulties dealing with IEDs. Second, empowerment is generating innovations throughout the world of the many and simple. In an example noted earlier, advanced manufacturing likely will first impact relatively simple applications. Empowerment has less impact on the few and complicated, thus the balance will favor the many and simple in the future.

The challenge for states with plentiful resources to devote to security is to leverage the innovations coming from the world of the many and simple. Security investments in the few and complicated are unlikely to disappear, since these investments provide advantages that resource-constrained actors cannot afford, thereby providing well-resourced actors an asymmetric advantage. The risk is that well-resourced nations may ignore the many and simple innovations to their detriment. They may end up expending resources in areas where open innovation provides free tools. They may ignore many and simple threats that have the potential to neutralize their few and complicated systems.

UAVs are a useful example of this trend. Current U.S. capabilities include systems like the Predator. Although not as complicated as systems like F-22s and B-2s, they are hardly simple. Empowerment, however, is favoring simple UAVs like the kind Austin Haughwout used to make his flying gun. The U.S. Naval Research Laboratory is looking at leveraging similar types of expendable UAVs to create drone swarms. The Predator operates in low-complexity environments where it is used against a handful of targets, while a drone swarm would generate a complex environment where it would be difficult to defend against the swarm, difficult to predict what the swarm was doing, and difficult to manage the battlefield. Even today, an adversary could purchase a sizable swarm of drones on the open market, challenging well-resourced militaries.

3.3 Expansion of Security beyond Government[23]



Global Implications — Security Impacts

Empowerment Spreads Responsibility

- Increased security demands beyond governments'
- Industry increasingly steward of security
  - Voluntary when interests align
  - Otherwise, carrots and sticks
- Empowerment allows independent actors to provide security
  - Open platforms provide tools
  - Governments cannot control
- Democratization of violence erodes state's monopoly on violence

Executives of Yahoo, AT&T, and Facebook Discuss Surveillance

Anonymous "Hacktivist" Group

Figure 11. Empowerment Spreads Responsibility for Security

Modern states usually hold a monopoly on the use of violence. They sometimes outsource this authority (e.g., security guards), but states still hold the ultimate decision rights. Technology empowerment is likely to exacerbate the "democratization of the tools of violence" (FitzGerald and Saylor, 2014, p. 19) in which more and more people will have the ability to engage in violence (Figure 11). Some worry that this democratization of violence will erode the legitimacy of governments (Wittes and Blum, 2015). In his study of the violence across history, which found that violence has been declining over time, Steven Pinker (2011) found that the state's monopoly on violence and provision of security "may be the most consistent violence-reducer." Therefore, the democratization of violence may exacerbate violence by eroding states' monopoly on violence.

[23] Image Credits: **Obama and Tech Executives**: President Obama at meeting with executives from leading tech companies at the White House in Washington December 17, 2013. Pictured are (L-R): Zynga co-founder Mark Pincus, Yahoo CEO Marissa Mayer, Obama, AT&T Chairman and CEO Randall Stephenson and Facebook COO Sheryl Sandberg. Pictured are (L-R): Zynga co-founder Mark Pincus, Yahoo CEO Marissa Mayer, Obama, AT&T Chairman and CEO Randall Stephenson and Facebook COO Sheryl Sandberg. Reuters/Kevin Lamarque. **Anonymous**: By Anonymous group [Public domain], via Wikimedia Commons; https://upload.wikimedia.org/wikipedia/commons/f/f8/We_are_anonymous_and_mask.jpg.

Wittes and Blum (2015) call the dispersal of the tools and authority for violence into the hands of non-government actors "distributed defense". Empowered individuals and groups are likely to engage in violence traditionally reserved to the state by either working alongside states (e.g., security guards) or working independently of states. Wittes and Blum find that outsourcing of violence most often occurs in weak states. For example, the United States in its early days had a weak Army and a weak Navy so had to rely on militias and privateers to act on its behalf.

There is currently much debate about distributed defense in the cyber realm. Although U.S. government efforts led to the Internet, cyber infrastructure is mostly privately owned. This is not unique—other network infrastructures,[24] like power distribution and telephone lines, are privately owned. However, these industries have been regulated historically, while cyber networks are relatively new and less regulated. Just as with other privately-owned infrastructure, governments must rely on the private sector to participate in the provision of security.

Several observers have made recommendations about how governments can best regulate and leverage the cyber industry. For example, *The Economist* (2015a,b) encourages regulations so that vulnerabilities can be patched, increasing the liability of companies when their products do not work as intended (to incentivize them to provide security), and promoting a culture of openness about vulnerabilities. Elazari (2015) expands on the last recommendation, by recommending that governments legalize and fund private research that searches for vulnerabilities, while at the same time reorienting government towards fixing—rather than exploiting—vulnerabilities. Many companies have already transitioned to an open R&D model where hackers are empowered to discover vulnerabilities. For example, companies like Microsoft, Google, and Yahoo have bounty programs where hackers can make careers (or get job offers) from finding vulnerabilities in these companies' systems and reporting them so that they can be fixed (The Economist, 2015c).

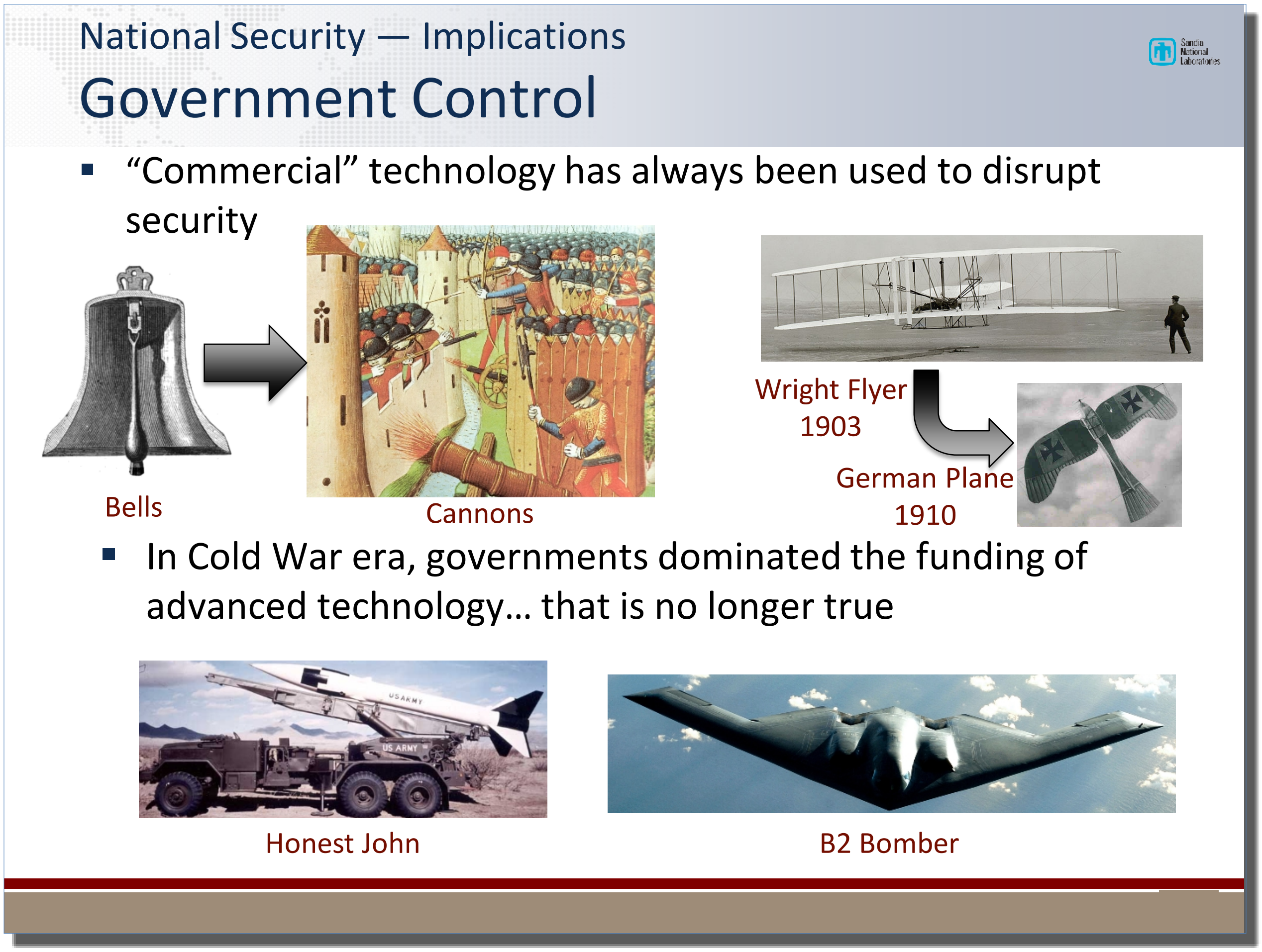
Government involvement in the cyber world does risk a backlash. Experts like Dan Geer (2013) fear that private companies and individuals are "compelled to become government agents" thus creating a "digital army of conscripts." Following the Edward Snowden affair, U.S. companies, fearing backlash from their customers in the United States and abroad, increased their rhetoric against U.S. government involvement, even going to the White House to scold the President. Apple's Chief Executive Officer, Tim Cook, has campaigned publicly against government limitations on encryption and against his rivals collection of user data (Moscaritolo, 2015).

Technology will also empower actors to work outside the interests of the state. This is clear in examples like IEDs or the Islamic State of Iraq and the Levant (ISIL), but it is also occurring within and across developed countries. For example, the hacktivist group Anonymous is a loosely affiliated group that conducts cyber-attacks on targets in ways that generally align with Western values, for example, by taking Jihadist websites offline (Goldman and Thompson, 2015). Although the interests of groups like Anonymous may sometimes overlap with the interests of governments, they also diverge. Even when interests align the methods that these groups use will run counter to state's interests in preserving their monopoly on violence.

[24] Network infrastructures have a high potential for externalities, where the actions of one owner can negatively impact other owners and users. They also have a high potential for monopoly. The potential for externalities and monopolies provides economic justification for government regulation.

Governments—especially those like the United States government that does not own much critical infrastructure—will need the support of industry and empowered individuals to coordinate the provision of distributed defense. To do this, governments need to demonstrate to the public the value of security. For example, Wittes and Blum (2015) argue that privacy, liberty, and security are usually complements, although much of the public debate is between tradeoffs that exist only at the margin. To obtain scarce funding for security, governments will also need to demonstrate the economic value of security by maximizing the benefits of defense R&D to non-defense industry (Gansler, 2011).

4 National Security Implications



National Security — Implications

Government Control

- "Commercial" technology has always been used to disrupt security
- In Cold War era, governments dominated the funding of advanced technology… that is no longer true

Bells
Cannons
Wright Flyer
1903
German Plane
1910
Honest John
B2 Bomber

Figure 12. Evolution of Government Control

Technology empowerment is changing the way in which researchers work. U.S. national security institutions will need to change to take advantage of the tools of empowerment and to maintain technical superiority over adversaries who will take advantage of these tools (Figure 12).

4.1 Defense Institutions Leverage Commercial Technology[25]

Traditionally, "commercial"[26] technology has been used by militaries, governments, and non-government actors to disrupt security. One popular, historic example is the case of church bells (Brodie and Brodie, 1973). In the 1300s, a few hundred years after church bell castings were invented, artisans discovered that they could use the same technologies to cast guns. "Siege Orleans," pictured above, is said to be the first depiction of a cannon used in battle at Joan of Arc's victory in Orleans during the Hundred Years War. It took about 200 years for the artisans to discover that they could reuse the molds and mass produce cannons, which reduced costs and further changed warfare.

The Cold War era was a unique time in which governments—especially the U.S. government—drove technological progress in a large number of areas directed primarily at security, but with occasional relevance to non-defense applications. Eisenhower's New Look policy emphasized nuclear weapons to offset the Warsaw Pact's superior numbers of soldiers. Once nuclear parity reduced this advantage, the Second Offset Strategy developed technologies like stealth, precision munitions, information, and the Global Positioning System to offset again the Warsaw Pact's quantitative advantages.

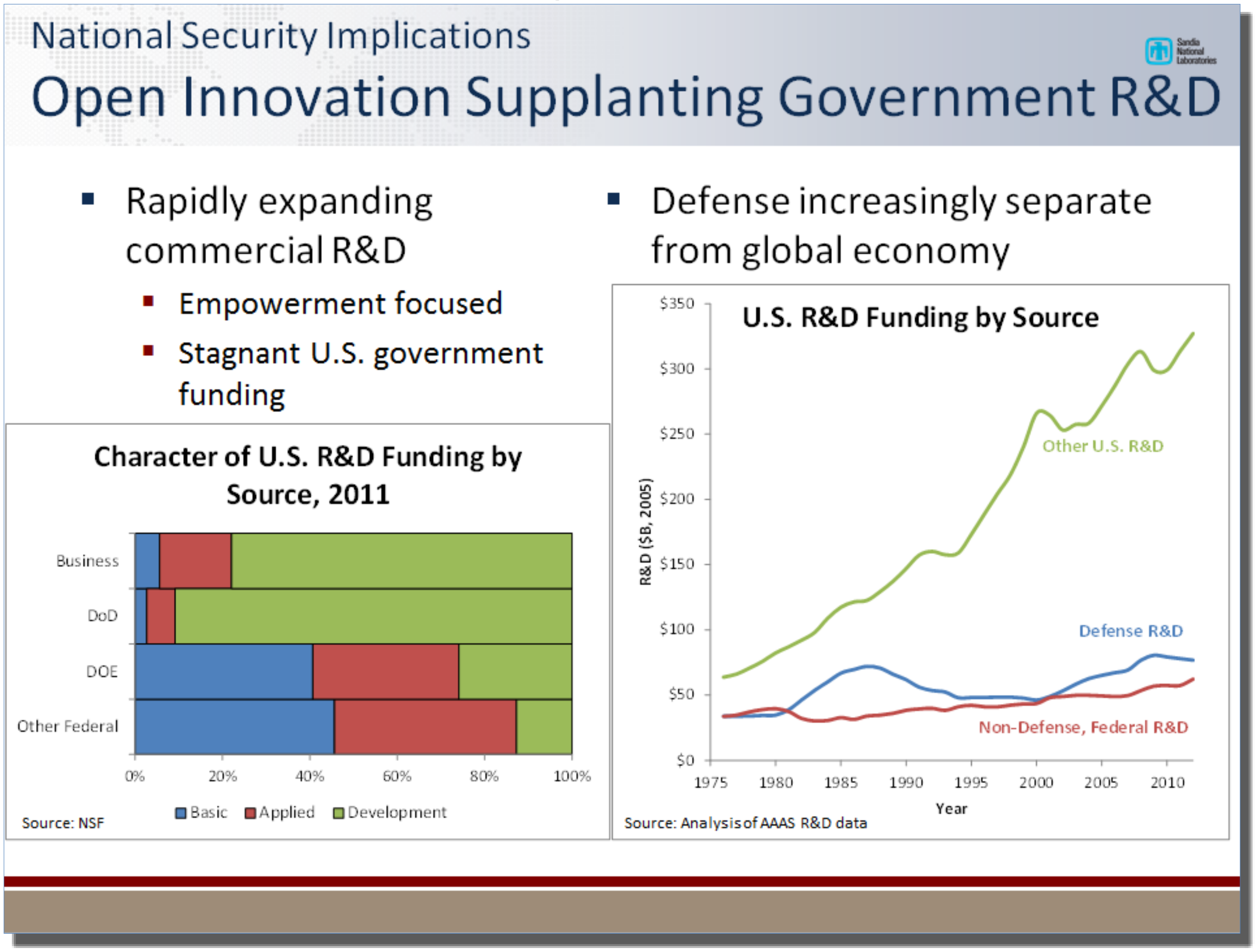
Even though technology was driven by governments seeking security during the Cold War, commercial technology still drove many of the technological advancements. For example, Krepinevich (1994) studied military revolutions throughout history and found that all the post-Industrial Revolution revolutions were "spinoffs". Chambers (2000) found that many of the most transformative technologies of the 20th Century (e.g., airplanes, tanks, radars, jet engines, helicopters, electronic computers) were not borne out of military need, although militaries funded R&D into these weapons systems to a much greater extent than in the past.

[25] Image Credits: **Church Bell**: By William Henry Stone [Public domain], via Wikimedia Commons, https://upload.wikimedia.org/wikipedia/commons/a/a6/Church_bell_cutaway.png
Cannons: "Siege Orleans". Licensed under Public Domain via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Siege_orleans.jpg#/media/File:Siege_orleans.jpg
Wright Flyer: "First flight2" by John T. Daniels - This image is available from the United States Library of Congress's Prints and Photographs division under the digital ID Full URL - http://www.loc.gov/pictures/resource/ppprs.00626/. Licensed under Public Domain via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:First_flight2.jpg#/media/File:First_flight2.jpg
German Bomber: Photo is from 1917, but model of plane is 1910. This was first used in Libya by shooting pistols or dropping grenades. "GermanFightingMonoplane1917" by Original uploader was Chris 73 at en.wikipedia - Transferred from en.wikipedia. Licensed under Public Domain via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:GermanFightingMonoplane1917.jpg#/media/File:GermanFightingMonoplane1917.jpg **"MGR-1 Honest John 05"** by U.S. Army - Redstone Arsenal Historical Informationhttp://www.redstone.army.mil/history/archives/missiles/honest_john_06.jpg. Licensed under Public Domain via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:MGR-1_Honest_John_05.jpg#/media/File:MGR-1_Honest_John_05.jpg
B2 Bomber: Val Gempis, USAF http://cdnph.upi.com/svc/sv/upi/8761402423712/2014/1/b4f112bc59515c48d6496da838dd1308/US-B-2-stealth-bombers-arrive-in-Europe.jpg),.

[26] By "commercial" we mean technologies and methods that are generally available to the public.

Commercial technologies have always disrupted security. It is likely that they will disrupt security to an even greater extent in the future as the pace of disruption increases from empowerment and governments reduce further from Cold War-era levels of defense investment.

4.2 U.S. Government R&D is Falling Behind[27]



National Security Implications

Open Innovation Supplanting Government R&D

- Rapidly expanding commercial R&D
  - Empowerment focused
  - Stagnant U.S. government funding
- Defense increasingly separate from global economy

Figure 13. U.S. Government is Becoming Relatively R&D Player

R&D funding from the U.S. government—both in defense and non-defense applications—has been relatively flat over the past 40 years. At the same, R&D funding by commercial industry has exploded, increasing more than five-fold during that time.

Funding from the U.S. Department of Defense (DoD) and commercial industry heavily favors development rather than basic or applied research. Non-defense government funding has traditionally dominated funding of U.S. basic and applied research, but industrial funding of basic R&D is drawing closer to federal funding ($15.1B vs. $29.1B) and industrial funding of applied R&D has surpassed federal funding ($43.9B vs. $29.1B).

[27] R&D analyses based on **American Association for the Advancement of Science (AAAS) data**: http://www.aaas.org/page/historical-trends-federal-rd; **National Science Foundation (NSF)**: National Science Foundation, National Center for Science and Engineering Statistics, Federal Funds for Research and Development (Fiscal Years [FY] 2010–12).

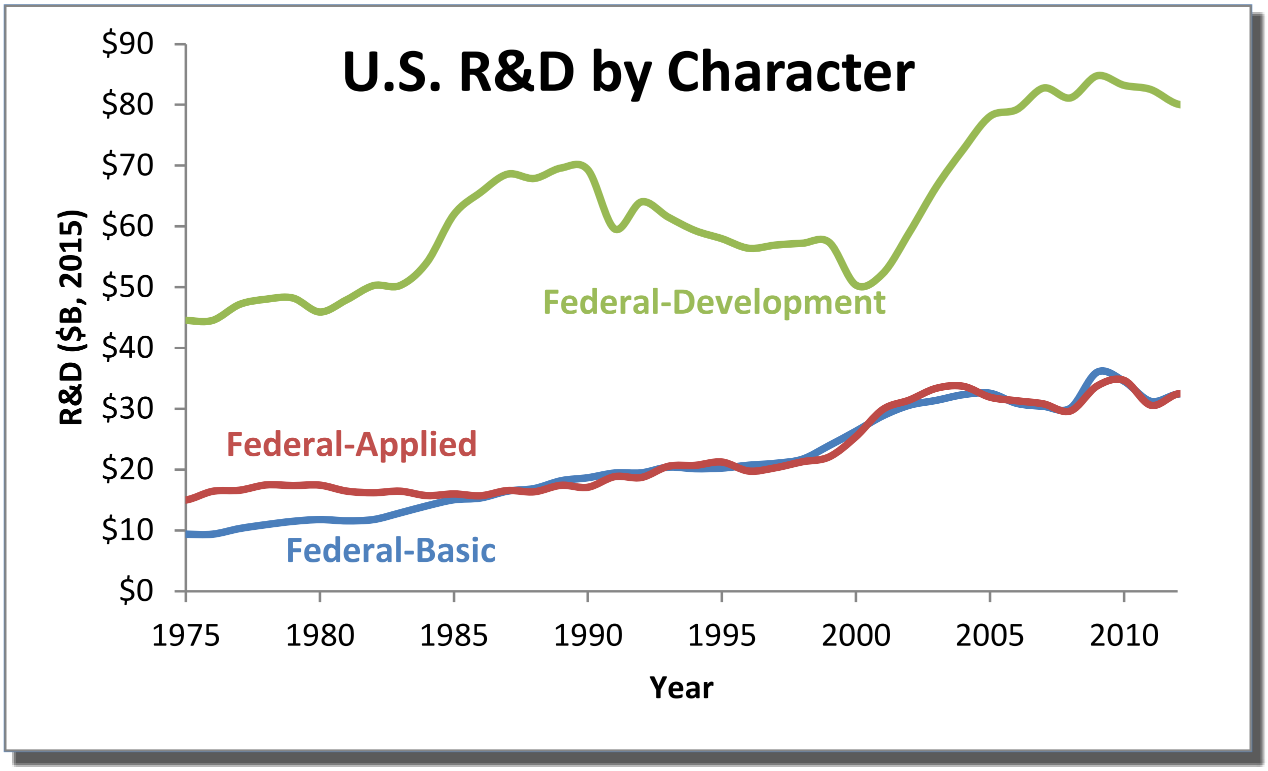
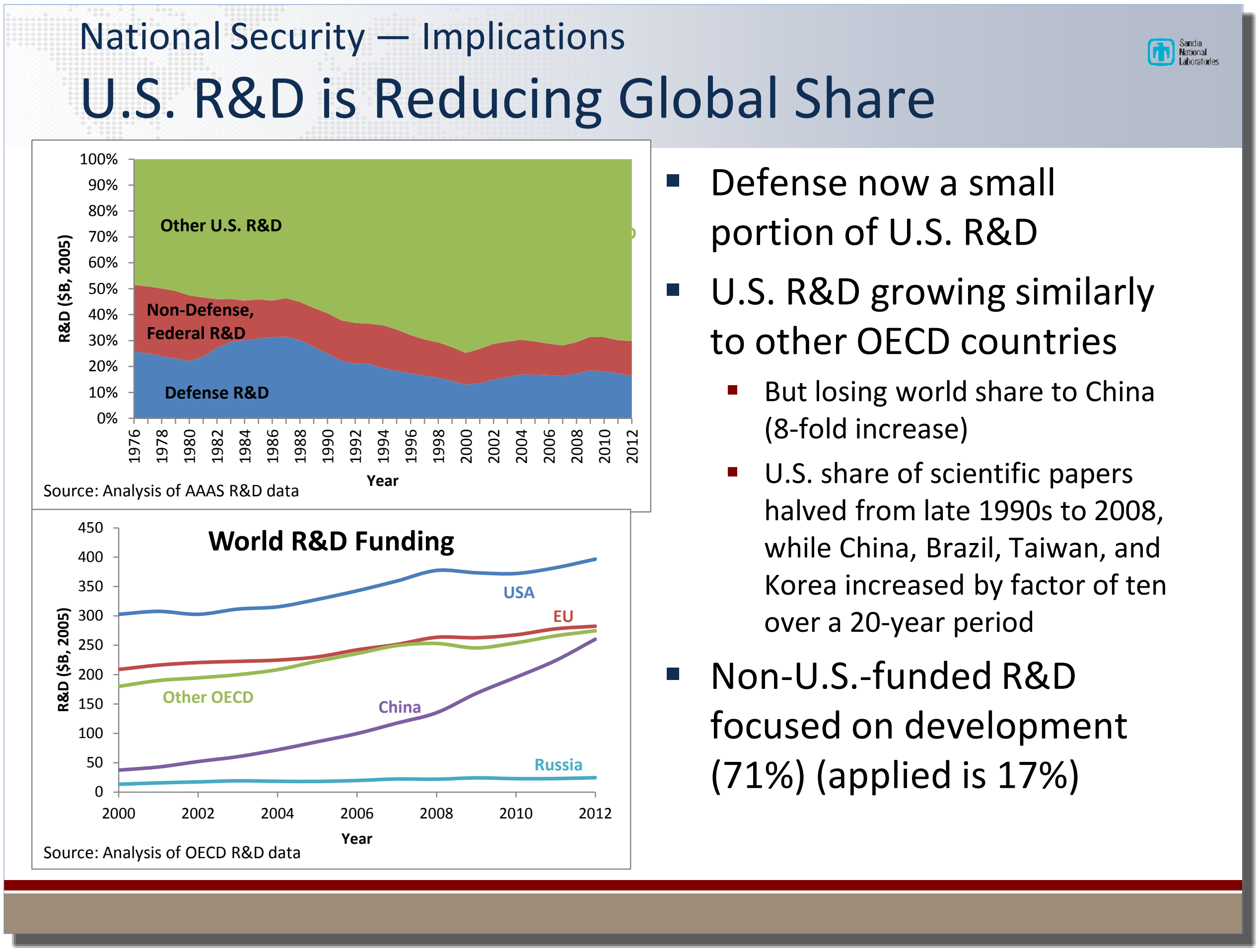


Figure 14. U.S. R&D by Character

As Figure 14 shows, federal funding of basic and applied research steadily grew to about 2004, while federal funding of development—driven by DoD—has followed similar patterns as the defense budget.



National Security — Implications

U.S. R&D is Reducing Global Share

Source: Analysis of AAAS R&D data

Source: Analysis of OECD R&D data

- Defense now a small portion of U.S. R&D
- U.S. R&D growing similarly to other OECD countries
  - But losing world share to China (8-fold increase)
  - U.S. share of scientific papers halved from late 1990s to 2008, while China, Brazil, Taiwan, and Korea increased by factor of ten over a 20-year period
- Non-U.S.-funded R&D focused on development (71%) (applied is 17%)

Figure 15. Falling U.S. Share of Global R&D

Despite strong growth in industry-funded R&D, the U.S. share of global R&D has been falling.[28] This is largely the result of the increase in R&D funding in China, which increased about eight-fold from 2000 to 2012 (Figure 15). Other indications, such as a declining share of scientific papers originating from the United States (Marsh, 2012) show that the United States is still the clear leader in global R&D, but other countries have been catching up. It is clear that the U.S. defense establishment is now a niche player in global R&D, whereas it historically funded a large share of global R&D.

Given the end of the Cold War, globalization, development, and the liberalization of formerly communist economies, it is unsurprising that the United States—and its defense establishments especially—have lost share of global R&D. Therefore, the data above do not by themselves justify worry. However, there is wide agreement that U.S. defense institutions are losing their competitive advantages as technology and innovation have diffused (Joint Chiefs of Staff, 2015). Jacques Gansler (2011) in his recent survey of defense institutions and the defense industry has

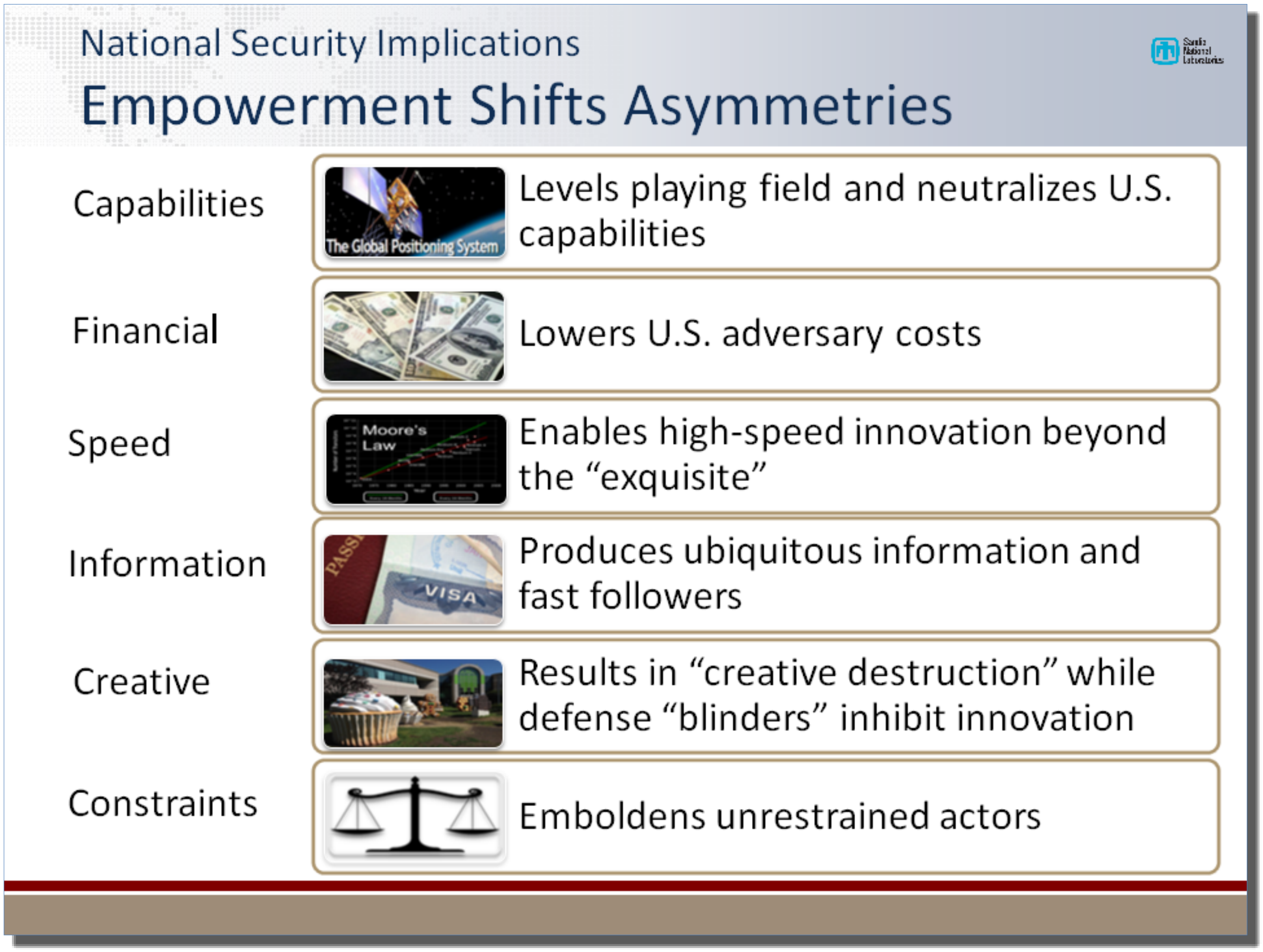
[28] Organization for Economic Cooperation and Development (OECD) data from http://stats.oecd.org/Index.aspx?DataSetCode=MSTI_PUB. “Other OECD” is estimated from OECD minus United States of America (USA) and European Union (EU). Some small EU countries are not in the OECD, so “Other OECD” is slightly underestimated.

summarized a large amount of research that shows that defense is falling behind. Gansler accuses defense institutions of being "autarkic" as they have failed to become more globally connected even as "globalization has achieved a great deal of technological leveling" (p. 104) and have become increasing separated from the U.S. commercial industrial base after the Cold War even as commercial R&D and empowerment have exploded. Rather than decreasing barriers[29] between the defense industrial base and the rest of the world, he finds that barriers have been increasing as the media and Congress have overreacted to cases of illegality or insufficient oversight that are infrequent. Instead, he believes that Congress should focus on repairing "broad structural issues" that generate day-to-day dysfunction across defense institutions (p. 155).

Gansler (2011) further worries that defense institutions are unable to attract top talent. The shift of R&D to industry, which provides more opportunities for top talent in the commercial world, is a major driver for these recruiting challenges (p. 45). Another driver is that defense no longer represents "the leading edge of technology" and defense work is increasingly limited and stifling (e.g., scientists and engineers in the defense industry tend to work on a single defense program that lasts decades versus a much faster pace of turnover in commercial industry).

[29] Gansler categorizes these barriers (2011, pp. 140-142) as: "Specialized cost-accounting requirements" that are difficult for commercial firms to implement; "Disclosure of accurate, complete, and current cost data in price negotiations" that commercial firms are reluctant to make; "Risks of losing intellectual property" to the government; "Export-control provisions" that may limit the markets commercial firms can serve; "Budget uncertainties" that mean Congress, not customers, drive budgets; "Logistics support differences" that limit the number of versions that DoD uses; "The requirements process," which discourages trades to find best value; and "Profit policy," which minimizes firms' profit rather than maximizing customers' value.

4.3 Empowerment is Shifting Asymmetries to Disadvantage U.S. National Security



National Security Implications

Empowerment Shifts Asymmetries

Capabilities	Levels playing field and neutralizes U.S. capabilities
Financial	Lowers U.S. adversary costs
Speed	Enables high-speed innovation beyond the “exquisite”
Information	Produces ubiquitous information and fast followers
Creative	Results in “creative destruction” while defense “blinders” inhibit innovation
Constraints	Emboldens unrestrained actors

Figure 16. Empowerment Erodes U.S. Advantages

Technology empowerment is reducing some asymmetries that advantage the United States while exacerbating asymmetries that disadvantage the United States. The following sections detail a variety of ways in which empowerment is disadvantaging the United States.

4.3.1 Empowerment is Eroding the U.S. Capability Advantage

At the core of U.S. national security strategy is the “differentiating strategy” of providing U.S. forces with “technological superiority” as an asymmetric advantage over potential adversaries. Former Secretary of Defense Robert Gates called these technologies “exquisite.”[30] As we saw in the IED example, technology empowerment has the ability to neutralize quickly U.S. capability advantages—adversaries discover new and creative ways to accomplish their goals and communicate them to others who build on those techniques (Figure 16). Furthermore, the tools of empowerment are available to everybody thereby leveling the playing field. For example, a hacker on an ordinary computer has the ability to discover highly consequential cyber vulnerabilities.

[30] See http://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1341 and http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=4404.

4.3.2 Empowerment is Eroding U.S. Financial Advantages

Throughout the Cold War, the size and health of the U.S. economy gave the United States the ability to outspend its rivals to increase capabilities and purchase large numbers of exquisite systems. Since the Cold War, other demands on funding have increasingly challenged U.S. defense budgets, decreasing the U.S. financial advantage. Furthermore, other countries—most notably China, whose economy is likely to someday surpass the size of the U.S. economy—have increasingly turned to markets and globalization to increase their ability to grow government budgets. Empowerment is pushing innovation to favor actors with fewer resources and thereby further neutralizing U.S. financial advantages.

In the future, the United States is still likely to leverage its financial advantage in technologies that empowered actors still cannot afford (e.g., directed energy) (FitzGerald and Saylor, 2014). The risk for U.S. national security is using these financial advantages to fund high-cost investments that can easily be countered by low-cost investments by adversaries (e.g., IEDs). Moreover, the United States is at risk of wasting high-cost investments to duplicate tools and innovations that empowerment has made available to all at a low cost.

The Defense Science Board (2013) recommends that the United States increase investments in "cost-imposing strategies" that cost more for adversaries to counter than it costs for the United States to employ. These investments could leverage U.S. financial advantages by developing technologies with relatively high, fixed development costs that only the United States or near-peers could afford, but have low costs of use that would provide the United States with a cost advantage.

4.3.3 Empowerment is Increasing the Importance of Speed

Exquisite technologies take a long time to develop. Commercial technologies—and technologies of empowerment, especially—develop at a rapid pace. Smart phones and their applications, for example, have changed the world in less than ten years. In the past decades, generally, the pace of development of exquisite defense technologies has slowed while the pace of commercial development has become faster.[31]

If exquisite technologies take years to develop but can be countered quickly by empowered actors, they will provide only an ephemeral advantage to the United States.

4.3.4 Empowerment Spreads Information that Anyone Can Access

Open innovation and empowerment relies on connectivity and accessibility. To innovate, empowered actors spread information. Unlike closed innovation systems, information in open innovation systems is born in the public.

In addition, empowerment increases threats to closely held information produced within closed innovation systems. The tools of empowerment have also made it easier for empowered actors to learn the secrets and tricks of the trade that were formerly secret or closely held in closed innovation systems. When this information escapes, it disseminates across networks and cannot be retracted.

[31] Gansler (2011, p. 210) finds that defense development time increased by about a third from 1969 to 1998. In the automobile industry, by comparison, development time decreased from 90 months to 24 months during that time.

This ubiquity of information provides an advantage to fast followers who can leverage the product of others' research but do not have to invest in that research, to the disadvantage of countries like the United States that spend large sums of money to develop the information.

4.3.5 Empowerment Increases the Importance of Creativity

Creativity is an important ingredient for generating tech-application surprise in an empowered world. Bunker (2015) says that traditional ways of thinking within the defense industry hamstring its workers with "blinders" and recommends that defense analysts look beyond the defense industry (for example, to artists, kids, and criminals with different perspectives) when trying to anticipate creative, unexpected uses of technology. The barriers between the defense and commercial worlds that Gansler discusses in his book are another set of blinders that cause defense "to view itself as different" and ignore technological innovation and surprises from commercial industry and empowered actors across the globe (Gansler, 2011, p. 53).

In his study of military revolutions, Krepinevich (1994) finds that the actors who lead the revolution are often not the best resourced, but they are creative and able to "substitute intellectual breakthroughs and organizational innovations for material resources." Similarly, Gregory Treverton (2015), Director of the National Intelligence Council has found that "Failure of national security is not a failure of intelligence or engineering, but of imagination."

Commercial industry and empowered actors have incentives to be creative. "Creative destruction" is the idea that organizations must be creative, otherwise more creative organizations will change industries and result in the destruction of incumbents. Empowered actors who participate in open innovation must be creative so that others adopt their ideas. If actors in open innovation networks fail to be creative, they will be pushed to the fringes rather than serving as important central nodes. Outside of a crisis, government institutions usually do not face the same incentives to be creative. As Singer and Cole (2015) note, companies like Google have organized to empower young, creative personnel with disruptive ideas, while defense personnel systems have remained the same for decades.

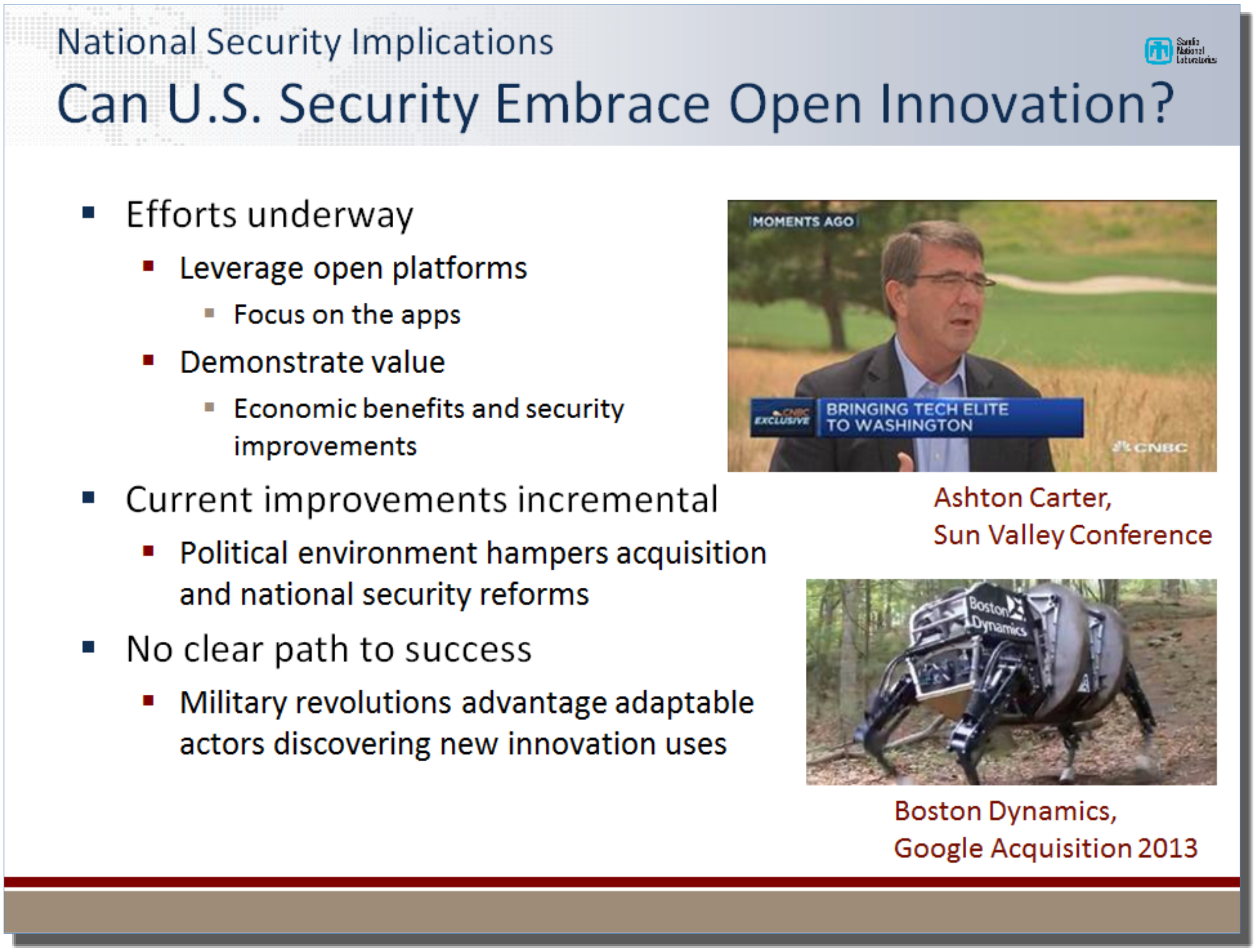
4.3.6 Empowerment Advantages Unconstrained Actors

States are usually more constrained in their behavior than empowered actors. For example, they usually try to follow international law and norms. Different states are also subject to different constraints. For example, as a hegemon encouraging adoption of liberal, Western values, the United States is particularly constrained by its "moral constraints and societal values" (FitzGerald and Saylor, 2014, p. 10).

These constraints limit the ability for the United States to experiment and innovate. There is substantial debate about whether and to what extent nations should invest in technologies and platforms,[32] but empowered actors such as Austin Haughwout can legally make a flying gun without any need for approval or debate. This means that empowered actors are likely to innovate in areas that the United States is reluctant to operate or experiment.

[32] For example, there is a substantial debate about the degree of autonomy that should autonomous weapons should be allowed (see the Future of Life Institute's open letter against autonomous robots, http://futureoflife.org/AI/open_letter_autonomous_weapons).

4.4 Open Innovation Will Force U.S. National Security to Change, but Change Will Be Difficult



National Security Implications

Can U.S. Security Embrace Open Innovation?

- Efforts underway
  - Leverage open platforms
    - Focus on the apps
  - Demonstrate value
    - Economic benefits and security improvements
- Current improvements incremental
  - Political environment hampers acquisition and national security reforms
- No clear path to success
  - Military revolutions advantage adaptable actors discovering new innovation uses

Ashton Carter,
Sun Valley Conference

Boston Dynamics,
Google Acquisition 2013

Figure 17. U.S. Security Policy Shifting Toward Open Innovation[33]

DoD has recently been engaging in efforts to better integrate with the commercial world and link to the tools of empowerment (Figure 17). For example, DoD is establishing the Defense Innovation Unit Experimental (DIUX) at Moffett Field in Silicon Valley to provide a link to the talent and technology in Silicon Valley (Tucker, 2015). Secretary of Defense Ashton Carter has been promoting ways to bring Silicon Valley talent to Washington to work with DoD for short rotations. DoD is establishing a third offset strategy through efforts such as the Defense Innovation Initiative and Long-Range Research and Development Initiative that are likely to tap into commercial technology and the tools of empowerment.

Researchers and policymakers have been advocating for fundamental acquisition and national security reform for over fifty years. The current efforts to integrate with commercial industry and

[33] Image Credits: **Ashton Carter at Sun Valley event to court tech industry** (http://media2.s-nbcnews.com/j/MSNBC/Components/Video/__NEW/_CNBC/c_closingbell_defensesec_150709.nbcnews-fp-360-200.jpg).
Boston Dynamics Legged Squad Support System: http://i.huffpost.com/gen/1372719/images/o-BOSTON-DYNAMICS-facebook.jpg.

the tools of empowerment are relatively incremental reforms that can be driven through DoD without approval or strong support from Congress. Therefore, researchers and analysts are pessimistic about the potential for reform. For example, Gansler (2011, pp. 52-54) describes how scandals during the 2000s led to an increase in procurement regulations, which separated defense further from commercial industry. FitzGerald and Saylor (2014, pp. 13-14) describe the situation as "The Unchanging Government Environment" where creative destruction does not apply and "Archaic regulatory barriers, distributive politics and entrenched interests have combined to forestall necessary change and protect favored capabilities."

A recent example that illustrates this pessimism is that of Boston Dynamics, a designer of animal- and human-like robots that focused on defense work for U.S. government.[34] In 2013, Google acquired Boston Dynamics and signaled that it would honor its existing government contracts, but not enter into new ones (FitzGerald and Saylor, p. 16). Google has even turned down government money for participating in the Defense Advanced Research Projects Agency (DARPA) Robotics Challenge (Sevcik, 2014).[35]

A first step in reform is likely reducing the various barriers that Gansler (2011) describes that discourage commercial companies from working with the U.S. government. At a minimum, this should discourage companies like Google from having a complete moratorium on entering into government contracts. Singer and Cole (2015) believe that defense institutions have a long and difficult path to forge enduring relationships with industry; the gulf has been growing with recent events, and defense institutions will have to demonstrate that closer relationships will benefit industry. Moreover, breaking down the barriers (though unlikely) may not be sufficient to ensure sufficient integration. For example, the Defense Science Board (2013, p. 79) says that if U.S. national security is to maintain technological superiority it must adopt "innovation enablers that allow it to anticipate, assess, and gain experience with new technological capabilities before its potential adversaries."

It will be difficult to achieve a high-level of integration between the U.S. government and commercial industry, which uses the tools of empowerment. Researchers have identified a number of barriers that have historically made this a rocky and unclear path. For example, in his studies of military revolutions, Krepinevich (1994) found that militaries are traditionally bureaucratic organizations that have difficulty adapting to new technology developments from the civilian world.[36] Many military revolutions are built by ambitious, adaptable powers that

[34] Sandia National Laboratories also reportedly worked with Boston Dynamics (Mick, 2014).

[35] Since this presentation was first given, Google (now called Alphabet, Inc.) has signaled that it will sell Boston Dynamics (Stone and Clark, 2016). Google is shifting its focus on nearer-term revenue, but Boston Dynamics is working on longer term projects without immediate revenue (a problem that was probably exacerbated by refusing government work). This nearer-term focus did not fit with Boston Dynamic's culture. Also, Google expressed discomfort when a video showing Boston Dynamic's humanoid robots went viral, since the humanoids appeared "terrifying."

[36] A classic example of bureaucratic complacency within militaries is the case of Gunfire at Sea (Morrison, 1966). The British Navy had discovered methods for dramatically increasing the accuracy of gunfire from a rolling ship at sea. However, complacency within the United States pushed back on adopting these methods until President Theodore Roosevelt became involved. Morrison explained this reluctance: "The opposition, where it occurs, of the soldier and sailor to [innovation] springs from the normal human instinct to protect oneself, and, more especially, one's way of life. Military organizations are societies built around and upon the prevailing weapons systems. Intuitively and quite correctly the military man feels that a change in weapons portends a change in the

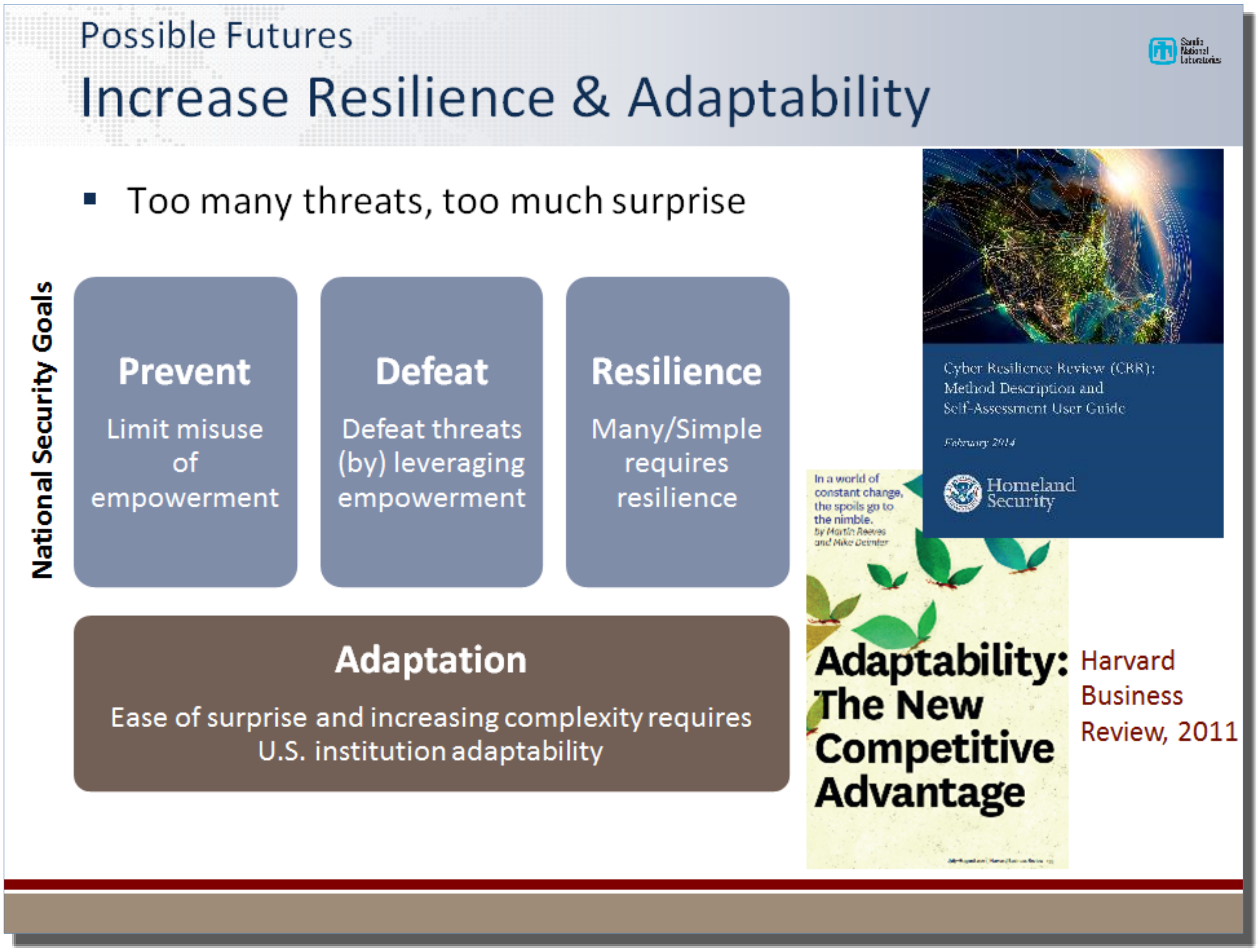
develop new concepts and ways of organization to take advantage of these technology advances. These adaptable powers are not necessarily the most powerful or most resource-rich nations, thus their ability to adapt to new technology can place established powers “at a severe competitive disadvantage”.[37] Davies (2015) similarly believes that hegemons tend to keep innovation in check because ruling elites are resistant to changes that could jeopardize their power; on the other hand, ambitious regimes have a greater incentive to encourage innovation to gain competitive advantages over other regimes. If the United States is unable to adapt to take advantage of the innovations enabled by technologies of empowerment, other ambitious nations or groups might instead discover how to leverage these technologies and obtain a competitive advantage over the United States.

A final note of caution about the difficulties of integrating defense with the rest of the economy comes from the historic failures of defense conversion. Adelman and Augustine (1992) contend that the only successful examples of defense industry converting to commercial industry up to that time were post-World War II Japan and Germany. They believe that the fundamental difficulties in integrating defense and commercial industry is that “defense work has little in common with commercial work” and that the culture in government and defense organizations becomes antithetical to working in the commercial world. Due to the importance of national security, defense and government organizations commonly employ the best and the brightest personnel, thus Adelman and Augustine recommend that governments preserve these capabilities but “bulldoze the corporate culture” and “bulldoze the management” to remove the barriers to integration.

arrangements of his society.”

[37] Krepinevich cites several examples: Guns had been available for a long time, but it was not until the 1400s that improvements to gunpowder and longer guns triggered widespread adoption of guns, which advantaged states over the nobility. France led early progress in submarines, but Germany in World War I figured out how to use submarines effectively. The United States first developed airplanes, but fell behind Europe in military use during World War I. The U.S. tank in the 1920s was copied by the Soviets, but during World War II the United States relied upon the Sherman Tank, which was inferior to the Soviets’ T-34. The United Kingdom, France, and Germany had access to similar technology before World War II. Only Germany created new concepts to integrate the technology effectively, which allowed them to conquer most of Western Europe in weeks.

5 Conclusion: Possible Futures



Possible Futures

Increase Resilience & Adaptability

- Too many threats, too much surprise

National Security Goals

Prevent Limit misuse of empowerment

Defeat Defeat threats (by) leveraging empowerment

Resilience Many/Simple requires resilience

Adaptation Ease of surprise and increasing complexity requires U.S. institution adaptability

Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide
February 2014
Homeland Security
In a world of constant change, the spoils go to the nimble.
by Martin Reeves and Mike Deimler
Adaptability: The New Competitive Advantage
Harvard Business Review, 2011

Figure 18. Future U.S. National Security Goals

This section concludes the report by looking at the goals that national security institutions must fill in the future and asking how institutions can become more adaptable to better promote national security.

5.1 Increased Importance of Resilience and Adaptability

National security policies and institutions typically try to reduce national security risks by either preventing bad things from happening and defeating threats when they emerge. There is growing recognition that resilience—that is, the ability for society and institutions to function during and following a disruptive event (or set of events)[38]—is becoming more important (Figure 18). To accomplish these goals, U.S. institutions will need to become more adaptable so they can leverage the tools of empowerment.

[38] This definition is based on the definition from Biringer, et al. (2013, p. 107): "Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is that system's ability to reduce efficiently both the magnitude and duration of the deviation from targeted system performance levels."

5.1.1 Prevent

A key national security goal is to prevent bad things from happening. In risk terms, it is to reduce the likelihood of a threat emerging. The 2015 U.S. *National Security Strategy* (Obama, 2015) emphasizes the importance of prevention across a number of different domains (i.e., prevention of terrorism, prevention of conflict, prevention of the spread and use of weapons of mass destruction). Prevention tends to be a focus of government organizations like the intelligence community, the State Department, and foreign military assistance. Technology empowerment will create additional threats that will need to be prevented (e.g., flying guns used in malicious ways), but it will also increase the difficulty of prevention as the democratization of the tools of violence spreads increasingly capable tools to more people and groups.

5.1.2 Defeat

When threats cannot be prevented, the goal of national security becomes defeating the threat so they cannot impose consequences on U.S. interests. In risk terms, the goal of defeat is to reduce the likelihood that of a threat that has emerged from imposing consequences. The 2015 U.S. National Security Strategy (Obama, 2015) states that the primary purpose of U.S. military forces is to "defeat and deny aggression." Technology empowerment complicates U.S. forces' ability to impose defeat by giving potential adversaries better technology, and more importantly the increased ability to innovate quickly to counter U.S. forces' capabilities and tactics. However, if U.S. forces can successfully leverage technology empowerment, the tools of empowerment will also enhance the ability of U.S. forces to defeat adversaries and innovate quickly to counter unexpected changes on the battlefield.

5.1.3 Resilience

Ever since the Department of Homeland Security (DHS) was stood up, and especially in the years after Hurricane Katrina in 2005, there has been an increased awareness of the importance of resilience.[39] In risk terms, resilience is the ability to reduce the consequences of a threat that has emerged and could not be defeated.

The true origins of resilience in U.S. national security probably emerged at least as far back as the Office of Civilian Defense during World War II, which was revived as the Federal Civil Defense Administration when the Soviet Union developed an atomic bomb. This later became part of the Office of Civil and Defense Mobilization, later the Office of Emergency Planning, later the Defense Civil Preparedness Agency, which became part of the Federal Emergency Management Agency (FEMA) upon creation in 1979.[40]

The 2015 U.S. National Security Strategy (Obama, 2015) sees resilience as a primary role for homeland security. However, as the tools of empowerment put more capability and innovation potential into the hand of a greater number of actors, national security threats will become harder to prevent and defeat. Therefore, the importance of resilience across national security institutions is likely to grow.

[39] The Cyber Resilience Review (CRR) is an example of one of the efforts to increase resilience in U.S. infrastructure. Image Credit: "CRR Self-Assessment User Guide" by US Department of Homeland Security - US Department of Homeland Security. Licensed under Public Domain via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:CRR_Self-Assessment_User_Guide.jpg#/media/File:CRR_Self-Assessment_User_Guide.jpg.

[40] For a history of FEMA, see http://www.fema.gov/about-agency.

5.1.4 Adaptability

The increased volatility of national security brought about by technology empowerment will demand greater adaptability of U.S. institutions if the United States is to be successful at minimizing national security risk through prevention, defeat, and resilience.

In the past decades, the business world has become more volatile as technology and globalization have advanced and the pace of innovation has increased. The volatility has demanded increased adaptability of companies to deal with this change. In the less volatile past the ability to be "really good at doing one particular thing" was most important for companies, but now companies must be adaptable by being "really good at learning how to do new things" (Reeves and Deimler, 2011). Similarly, during the Cold War the certainty and simplicity of the bilateral relationship with the Soviet Union meant that the United States needed a few exquisite capabilities to maintain its advantage, but in today's much more volatile, unpredictable, and complex security landscape U.S. security institutions must be adaptable to be successful.

Adaptability is easier said than done, especially for institutions that have existed for decades without needing to be particularly adaptable. Nevertheless, some common themes exist about how U.S. institutions might become more adaptable.

Experimentation: Probably the most important factor in creating an adaptable institution is instilling an ability to experiment. The technologies of empowerment increase the pace of innovation so quickly because they empower people to engage in experiments to learn about how the world works. Similarly, adaptive companies leverage experimentation to better understand their markets and how they can innovate to serve them (Reeves and Deimler, 2011). Experimentation means failures, so "adaptive companies are very tolerant of failure, even to the point of celebrating it" (Reeves and Deimler, 2011, p. 139)—a culture that is antithetical to the risk aversion in government bureaucracies. Similarly, the Defense Science Board (2013, p. xxii) recommends experimentation to "explore, discover, analyze, and understand the potential of emerging technologies and their ability to enhance military capability and doctrine" to avoid and create surprise and challenge the "increasingly risk averse" defense environment. Gansler (2011, pp. 274-275) recommends getting technology out of the labs and to warfighters faster for experimentation so that "novel ideas" generated during the experiments can be used to guide the development and use of the technology.

Breaking Down Stovepipes: Coordination across an organization becomes increasingly difficult as an organization grows, so large organizations tend create stovepipes to manage coordination. Adaptable companies create the ability to work across corporate stovepipes by creating "environments that encourage the knowledge flow, diversity, autonomy, risk taking, sharing, and flexibility on which adaptation thrives" that move decisions to the front lines by "creating decentralized, fluid, and even competing organizational structures" that break rigid hierarchies (Reeves and Deimler, 2011, p. 140). Adaptable companies break down other corporate barriers by working with networks that include its suppliers and customers (Reeves and Deimler, 2011, pp. 139-140). Important future technologies are likely to involve synergies between seemingly unrelated technologies across disciplinary boundaries (Committee on Forecasting Future Disruptive Technologies, National Research Council, 2009), thus the preoccupation of government cost cutters with strengthening stovepipes by eliminating all perceived duplication of capabilities could further harm institutions' adaptability.

Analysis and Foresight: An adaptable company "must have its antennae tuned to the signals of change from the external environment, decode them, and quickly act to refine or reinvent its business model," (Reeves and Deimler, 2011, p. 138). Rather than making detailed plans for the next year, adaptive companies tend to engage in foresight activities that look decades out, but only make plans in the short-term (Laloux, 2014, p. 210).[41] Similarly, the Defense Science Board (2013, p. 71) recommends that defense institutions make "hedging" investments that enable monitoring of technology and to create opportunities to "take advantage of emerging opportunities in a timely way." They also recommend engaging in horizon scanning through "continuous monitoring of advancing technologies."

Increase Resources and Decrease Constraints: Adaptable companies enjoy a positive feedback system—when companies successful adapt, they tend to increase their profits, which gives them a greater freedom to act in the future. In general, defense institutions do not have the same set of positive feedbacks for resources because they ultimately rely on Congress for resources. Gansler (2011, p. 20) calls for defense policies that maximize the value of resources devoted to defense by reducing the costs of national security while finding ways for defense institutions "to strengthen the U.S. economy through dual-use investments in security and economic growth". As mentioned earlier, defense institutions are also subject to a wide variety of constraints. These constraints flow out of the fact that government funding and institutions are ultimately accountable to the people. As an example, Wittes and Blum (2015) advocate surveillance as a solution to the increased risks of technology empowerment. However, a limitation to using surveillance is an increasing amount of pushback, so they advocate that governments focus on engaging in surveillance[42] that people view as "just" by maximizing the public's perception of the benefits of surveillance and minimizing their perception of the costs.

5.2 Implications for U.S. Defense Institutions

If U.S. national security is to remain strong, U.S. institutions will need to embrace technology empowerment and the innovation it drives. To do this, U.S. institutions must become increasing adaptable so that they can learn how to improve continuously to respond to the increasing uncertainty and volatility of the future national security environment.

In this uncertain future, specific, concrete, and certain recommendations for investments and policies are decreasingly likely to exist. Instead, adaptable institutions must be equipped to deal with ambiguity and discover how to react quickly to changes in the world, and more importantly, become proactive about creating change to their advantage. This is a world where experimentation will be key, and failure will be an inevitable, common, but necessary feature of discovery.

[41] Laloux (2014, p. 210) likens this to thinking like a farmer, where investments in equipment and crops like fruit trees must anticipate the world decades out, but plans must adapt to fluctuations in weather.

[42] In reviewing the history of platform technologies, Wittes and Blum (2015) find that governments tend to focus on surveillance to provide security. For example, surveillance of Roman roads helped reduce banditry. Surveillance is appealing because it strengthens all three goals of national security—it aids prevention by discovering threats, it aids defeat by providing a deep understanding of the adversary, and it aids in resilience by providing a deep understanding of one's own society and infrastructure.

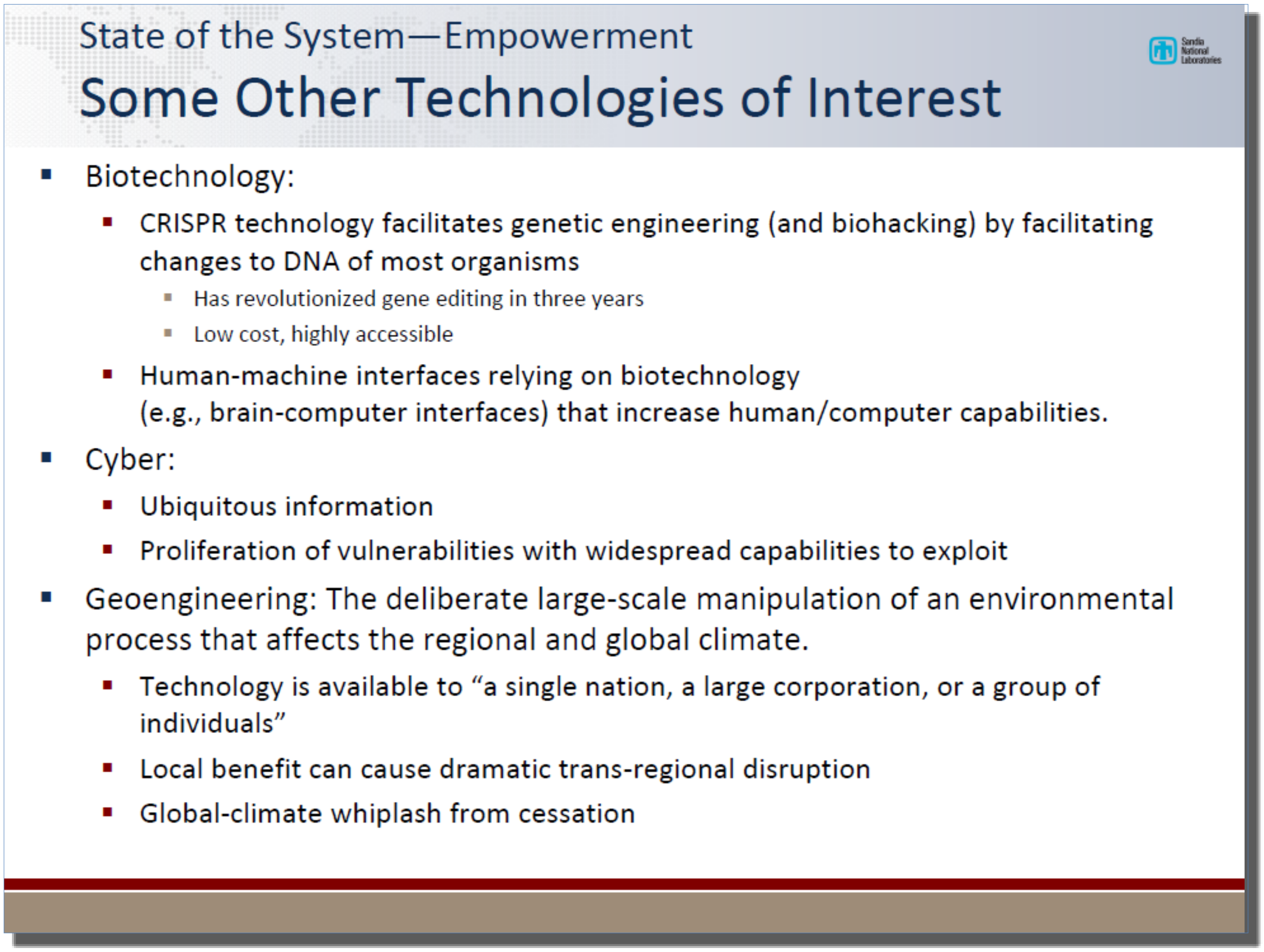
Our study suggests several areas for government institutions to focus. First, the shift from the few and complicated to the many and simple is likely to have large implications for national security, and may even usher in a new military revolution. The implications of these changes are not clear, but it is likely that both the United States and its potential adversaries will leverage the many and simple.

Another potential area of focus is open innovation. Empowered people and groups are innovating and creating technologies through open innovation that are essentially free. How can U.S. institutions leverage these innovations while maintaining capability advantages over potential adversaries?

U.S. institutions have a large number of constraints that make adaptability difficult. How can U.S. institutions become more adaptable in the face of these constraints? Do Federally Funded Research and Development Centers have advantages they can leverage due to their independence from the government but with access not afforded to typical government contractors?

Finally, how can institutions maximize their value to the nation, likely by engaging in work that breaks down traditional stovepipes, increases economic impact, and engages in technically-risky yet highly-impactful work?

Appendix A Other Technologies of Interest



State of the System—Empowerment

Some Other Technologies of Interest

- Biotechnology:
  - CRISPR technology facilitates genetic engineering (and biohacking) by facilitating changes to DNA of most organisms
    - Has revolutionized gene editing in three years
    - Low cost, highly accessible
  - Human-machine interfaces relying on biotechnology (e.g., brain-computer interfaces) that increase human/computer capabilities.
- Cyber:
  - Ubiquitous information
  - Proliferation of vulnerabilities with widespread capabilities to exploit
- Geoengineering: The deliberate large-scale manipulation of an environmental process that affects the regional and global climate.
  - Technology is available to "a single nation, a large corporation, or a group of individuals"
  - Local benefit can cause dramatic trans-regional disruption
  - Global-climate whiplash from cessation

Throughout the course of the study, researchers on the study team looked at many platforms and technologies in detail, and discussed these technologies with subject matter experts. In our research and discussions, several technologies stood out as being potentially high risk (i.e., relatively high consequence and high likelihood). Note, however, that the goal of this exploration was not identifying the highest risk technologies, but rather to explore the characteristics of these risks. Several of the technologies are discussed in the main presentations, but four additional technologies stood out and are worth mentioning.

Biotechnology

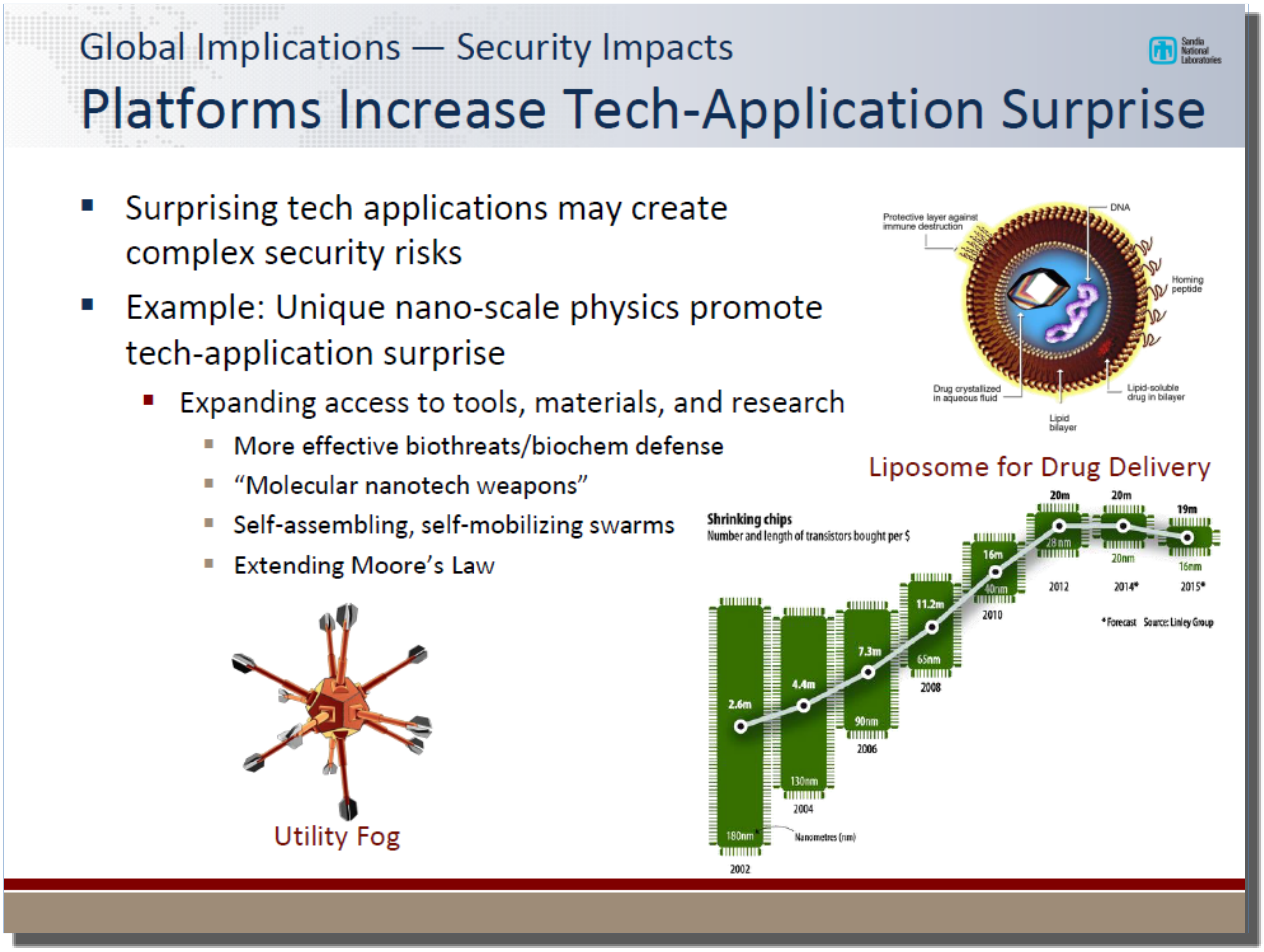
The first of the potential high-risk technologies is biotechnology. Recent advances in CRISPR in a few short years revolutionized gene editing so that it is much cheaper and accessible than previous gene editing techniques (see Ledford, 2015). By democratizing the ability to edit genes, the possible innovations and their impacts seem large and impactful. Another potentially high-impact biotechnology is human-machine interfaces. In particular, brain-machine interfaces have long been used in animal experimentation and in neuroprosthetics (e.g., cochlear implants for hearing) (Serruya, et al., 2002). However, in the future such interfaces are likely to become more common to augment human abilities, for example, in military applications (Chief Scientist of the United States Air Force, 2013, p. 21). The potential impact of biotechnology was so great that the Global Futures team decided to do a follow-on study exclusively on the future of biotechnology (Sumner, et al. 2016).

Cyber

The second technology is cyber, which combines networked computers with other technologies like robotics and artificial intelligence. As we discuss in the main report, cyber has been key to increasing connectivity and accessibility to enable technology empowerment. Cyber technology has been changing the world rapidly and will likely continue doing so in the future. This provides both new opportunities as well as new vulnerabilities and risks.

Geoengineering

The third high-risk technology is geoengineering. Geoengineering is more in its infancy than other technologies explored in this study, and the risks and opportunities have been studied less. However, geoengineering technology is already available that allows groups of individuals to manipulate regional climate (Committee on Geoengineering Climate, 2015, p. 25). For example, ships can release aerosols to increase the albedo of the ocean, thus reflecting the sun's energy away from earth.



Global Implications — Security Impacts

Platforms Increase Tech-Application Surprise

- Surprising tech applications may create complex security risks
- Example: Unique nano-scale physics promote tech-application surprise
  - Expanding access to tools, materials, and research
    - More effective biothreats/biochem defense
    - "Molecular nanotech weapons"
    - Self-assembling, self-mobilizing swarms
    - Extending Moore's Law

Protective layer against immune destruction
DNA
Homing peptide
Drug crystallized in aqueous fluid
Lipid bilayer
Lipid-soluble drug in bilayer

Liposome for Drug Delivery

*Forecast Source: Linley Group

Utility Fog

Nanotechnology

The fourth high-risk technology is nanotechnology, which is another platform that is likely to increase tech-application surprise. Nanotechnology, especially, can be combined with other platforms to create surprises. For example, DoD is conducting research into small "maple seed" reconnaissance vehicles (Gansler, 2011, p. 103) that combine robotics and artificial intelligence with nanotechnology in a small vehicle that propels itself by rotating like a falling maple seed. Nanotechnology can also be combined with biotechnology, for example, by creating liposomes to deliver drugs more effectively, as illustrated in the figure above (see Gold, 2014).[43] Futurists have envisioned one day being able to construct a utility fog of nano-machines[44] that could self-assemble to replicate physical structures.

Nanotechnology may lead to particularly surprising and impactful innovations because nanoscale physics are much different than at higher scales, but are not yet well understood. For example, nanoelectronics and nanomaterials might enable improvements in energy storage and computing density of 100-fold (Chief Scientist of the United States Air Force, 2013), which could potentially extend Moore's law further into the future.[45] On the other hand, these nanoscale properties could potentially lead to health and safety risks that are currently unknown (Hossain, 2014). As Table 1 shows, there is concern that the potential risk of nanotechnology could result in massive loss of human life or even extinction within this century.

Table 1. Estimates of Existential Risk by 2100

	≥1M Dead	≥1B Dead	Extinction
Molecular nanotech weapons	25%	10%	5%
Super intelligent Artificial Intelligence	10%	5%	5%
All Wars	98%	30%	4%
Engineered pandemic	30%	10%	2%
Nanotech accident	5%	1%	0.5%
Natural pandemic	60%	5%	0.05%
Nuclear terrorism	15%	1%	0.03%

Source: Oxford University Future of Humanity Institute (Sandberg and Bostrom, 2008)

[43] The liposome figure is from "Liposome". Licensed under Public Domain via Wikipedia - https://en.wikipedia.org/wiki/File:Liposome.jpg#/media/File:Liposome.jpg.

[44] The utility fog illustration is a 12-arm machine: "Foglet" by Steven Martin - Made myself using Cinema4D R8.. Licensed under Public Domain via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Foglet.jpg#/media/File:Foglet.jpg.

[45] The graph on the slide from the Economist Explains (2015) shows how Moore's law no longer appears to be holding when measured by cost. The increasingly high costs of producing such small transistors now outweighs their size advantages.

6 References

Adelman, Kenneth L. and Norman R. Augustine, 1992, "Defense Conversion: Bulldozing the Management," *Foreign Affairs*, v. 71(2), pp. 26-47.

Augustine, Norman R., 1979, "Augustine's Laws and Major System Development Programs," *Defense Systems Management Review*, v. 2(2), pp. 50-76.

Augustine, Norman R., 2015, "Augustine's Laws and Major System Development Programs," *Defense Systems Management Review*, v. 22(1), pp. 2-63.

Biringer, Betty, Eric Vugrin, and Drake Warren, 2013, *Critical Infrastructure System Security and Resiliency*, Boca Raton: CRC Press.

Brodie, Bernard and Fawn M. Brodie, 1973, *From Crossbow to H-Bomb, The Evolution of the Weapons and Tactics of Warfare*, Bloomington: Indiana University Press, Revised and Enlarged Edition.

Bunker, Robert J., 2015, "Criminal-Terrorist-Insurgent Unmanned Aerial Systems Use and Potentials", SOUTHCOM Area of Interest Presentation for Minerva Research Initiative, July 8, 2015

Carlson, J.M. and John Doyle, "Complexity and Robustness", *PNAS*, February 19, 2002, v. 99, pp. 2538-2545.

Chambers II, John Whiteclay, 2000, "Weaponry, Evolution of", *The Oxford Companion to American Military History*, encyclopedia.com, retrieved July 7, 2015.

Chief Scientist of the United States Air Force, 2013, *Global Horizons, Final Report, United States Air Force Global Science and Technology Vision*, AF/ST TR 13-01.

Committee on Forecasting Future Disruptive Technologies, National Research Council, 2009, *Persistent Forecasting of Disruptive Technologies*, Washington, D.C.: National Academies Press.

Committee on Geoengineering Climate: Technical Evaluation and Discussion of Impacts; Board on Atmospheric Sciences and Climate; Ocean Studies Board; Division on Earth and Life Studies; National Research Council, 2015, *Climate Intervention: Reflecting Sunlight to Cool Earth*, Washington: The National Academies Press.

Davies, Stephen, 2015, "Blood and Leviathan: A Stanford historian thinks war is the engine that drives civilization. Is he right?" *Reason*, July 2015.

Defense Science Board, 2013, *Technology and Innovation Enablers for Superiority in 2030,* October 2013, Washington: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.

Elazari, Keren, "How to Survive Cyberwar: Step One: Stop Counting on Others to Protect You," *Scientific American*, April 2015, pp. 66-69.

FitzGerald, Ben and Kelley Sayler, 2014, *Creative Disruption: Technology, Strategy and the Future of the Global Defense Industry*, Washington, D.C.: Center for a New American Security.

Gansler, Jacques S., 2011, *Democracy's Arsenal: Creating a Twenty-First-Century Defense Industry*, Cambridge: MIT Press.

Geer, Dan, 2013, "Tradeoffs in Cyber Security," Speech at UNC, October 9, 2013, http://geer.tinho.net/geer.uncc.9x13.txt.

Gold, Ian, 2014, "Future Global Trends in Innovation", in *Innovation: Managing Risk, not Avoiding It: Evidence and Case Studies, Annual Report of the Government Chief Scientific Advisor, 2014,* United Kingdom Government Office for Science, pp. 25-34.

Goldman, David and Mark Thompson, 2015, “Anonymous Blocks Jihadist Website in Retaliation for Charlie Hebdo Attack,” *CNN Money*, January 12, 2015, http://money.cnn.com/2015/01/11/technology/security/anonymous-charlie-hebdo/.

Government Accountability Office, 2012, “Counter-Improvised Explosive Devices: Multiple DOD Organizations are Developing Numerous Initiatives”, GAO-12,861R.

Hammes, T.X., 2014, “Future of Warfare: Small, Many, Smart vs. Few & Exquisite,” War on the Rocks, http://warontherocks.com/2014/07/the-future-of-warfare-small-many-smart-vs-few-exquisite/.

Harrison, Adam Jay, Jawad Rachami, and Christopher Zember, 2015, “Technology Domain Awareness: Building the Defense Innovation Base,” *Georgetown Security Studies Review*, v. 3(1), pp. 32-46.

Hossain, Kamal, 2014, “Nanomaterials”, in *Innovation: Managing Risk, not Avoiding It: Evidence and Case Studies*, United Kingdom Government Office for Science, pp. 54-55.

JIEDDO, 2012, Strategic Plan: Executive Summary, 2012-2016, https://www.jieddo.mil/content/docs/20120116_C-IEDStrategicPlan_ExSum_Final-Web.pdf.

Joint Chiefs of Staff, 2015, *The National Military Strategy of the United States of America, 2015: The United States Military’s Contribution to National Security*, June 2015.

Krepinevich, Andrew F., 1994, “Cavalry to Computer: The Pattern of Military Revolutions,” *The National Interest*, n. 37 (Fall 1994), pp. 30-42.

Laloux, Frederic, 2014, *Reinventing Organizations*, Brussels: Nelson Parker.

Ledford, Heidi, 2015, “CRISPR, The Disrupter”, *Nature*, v. 522, June 4, 2015, pp. 20-24.

Marsh, Peter, 2012, *The New Industrial Revolution: Consumers, Globalization and the End of Mass Production*, New Haven: Yale University Press.

Mick, Jason, 2014, “Google is Teaching Its Robots the Deadly Art of Karate (No, Really)”, DailyTech.com, November 11, 2014, http://www.dailytech.com/Google+is+Teaching+its+Robots+the+Deadly+Art+of+Karate+No+Really/article36874.htm.

Morrison, Elting E., 1966, *Men, Machines, and Modern Times*, Cambridge, MA: The MIT Press, pp. 17-44.

Moscaritolo, Angela, 2015, “Tim Cook Slams Rivals on Privacy, Data Collection,” *PC Magazine*, June 3, 2015, http://www.pcmag.com/article2/0,2817,2485279,00.asp

Naval Research Advisory Committee, 2009, “Disruptive Commercial Technologies”, http://www.nrac.navy.mil/docs/2009_Disruptive_Commercial_Technologies.ppt, accessed July 2, 2015.

Obama, Barack H., 2015, *National Security Strategy*, February 2015.

Pinker, Steven, 2011, *The Better Angels of Our Nature: Why Violence has Declined*, New York: Penguin Group.

Reeves, Marin and Mike Deimler, 2011, “Adaptability: The New Competitive Advantage,” *Harvard Business Review*, July-August 2011, pp. 135-141.

Sandberg, Anders and Nick Bostrom, 2008, *Global Catastrophic Risks Survey*, Technical Report #2008-1, Future of Humanity Institute, Oxford University, Oxford, England

Sevcik, J.C., 2014, “Google Rejects Military Funding in DARPA Robotics Challenge, Remains in Competition,” *UPI*, March 24, 2014, http://www.upi.com/Business_News/2014/03/24/Google-rejects-military-funding-for-DARPA-Robotics-Challenge-remains-in-competition/5441395686972/.

Simmons, Michael, 2015, "The No. 1 Predictor Of Career Success According To Network Science," *The Mission*, August 10, 2015, https://medium.com/the-mission/the-number-one-predictor-of-career-success-according-to-network-science.

Singer, P.W. and August Cole, 2015, "Flight Plan: The Government Needs to Work with Silicon Valley to Create our Military Future," *Slate*, August 27, 2015, http://www.slate.com/articles/technology/future_tense/2015/08/ghost_fleet_the_government_needs_to_work_with_silicon_valley_to_create_our.2.html.

Stone, Brad and Jack Clark, 2016, "Google Puts Boston Dynamics Up for Sale in Robotics Retreat," *Bloomberg*, March 17, 2016, http://www.bloomberg.com/news/articles/2016-03-17/google-is-said-to-put-boston-dynamics-robotics-unit-up-for-sale, (accessed April 5, 2016).

Sumner, Matthew, Thomas Nelson, George Backus, Patricia Pacheco, Brandon Heimer, Thor Osborn, and Wendell Jones, 2016, *Biotechnology: A Bio-Empowered World*, (presented within *Global Futures: Background and Biotech Brief*, Thomas Nelson and Matthew Sumner), SAND2016-4672 PE. Albuquerque, NM: Sandia National Laboratories.

Serruya, Mijail D., Nicholas G. Hatsopoulos, Liam Paninski, Matthew R. Fellows, and John P. Donoghue, 2002, "Brain-Machine Interface: Instant Neural Control of a Movement Signal," *Nature*, v. 416, pp. 141-142.

The Economist, 2015a, "Cyber-Security: Their Own Devices," *The Economist*, July 18, 2015.

The Economist, 2015b, "Embedded Computers: Hacking the Planet," *The Economist*, July 18, 2015.

The Economist, 2015c, "The Big Bug Hunt: It is Too Easy to Hack Into Websites, but Some People do so to Make it Harder," *The Economist*, August 1, 2015.

The Economist, 2015d, "Time to Fix Patents: Ideas Fuels the Economy. Today's Patent Systems are a Rotten Way of Rewarding Them," *The Economist*, August 8, 2015.

Treverton, Gregory F., Chairman of the National Intelligence Council, Comments during visit to Kirtland AFB, April 2, 2015.

Tucker, Patrick, 2015, "Pentagon Sets Up a Silicon Valley Outpost: Can Ash Carter Enlist a Tech Community Spooked by Spying and Allergic to Bureaucracy?" *Defense One*, April 23, 2015, http://www.defenseone.com/technology/2015/04/pentagon-sets-silicon-valley-outpost/110845/.

Wittes, Benjamin and Gabriella Blum, 2015, *The Future of Violence: Robots and Germs, Hackers and Drones, Confronting a New Age of Threat*, New York: Basic Books.

Distribution

1	MS0159	George Backus	0154 (electronic copy)
1	MS0159	Wendell Jones	0159 (electronic copy)
1	MS0159	Tom Nelson	0159 (electronic copy)
1	MS0159	Russ Skocypec	0159 (electronic copy)
1	MS0159	Drake Warren	0159 (electronic copy)
1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories